BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-224340

(43)Date of publication of application : 21.08.1998

(51)Int.Cl. H04L 9/08
H04Q 7/38
H04B 1/713
H04K 1/08

(21)Application number : 09-025456

(22)Date of filing : 07.02.1997

(71)Applicant : BROTHER IND LTD

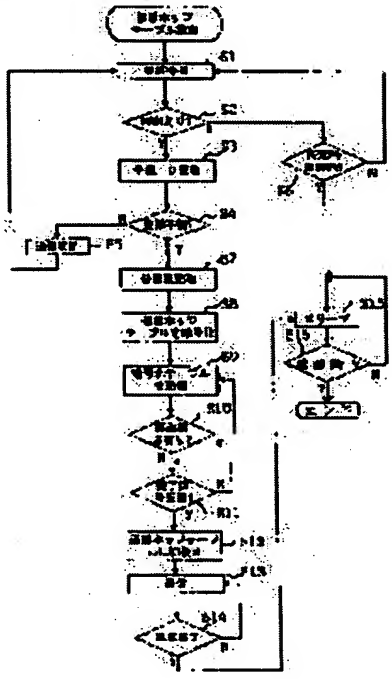
(72)Inventor : TAKI KAZUYA

(54) RADIO COMMUNICATION METHOD AND RADIO COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a radio communication method and a radio communication system in which secrecy of information to be sent/received between a master set and a specific slave set is enhanced.

SOLUTION: A master set encrypts a hop table in the frequency hopping system through the public key system (step S8) by using a public key from a slave set (step S7) and transmits the information to the slave set (step S9), the slave set uses a private key to decode the information and then both the master set and the slave set share the hop table in common and send/receive information by the frequency whipping system (step S13). Furthermore, both the master set and the slave set are provided with a hop table generator ad send/receives only an initial value encrypted by the public key encryption system and generate the hop table by using the initial value. Moreover, a password used to identify the slave set is encrypted by the public key encryption system and the master set and the slave set send/receive the password.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention belongs to the technical field of the radio method which delivers and receives the information concerned, and a radio communications system in the radio between a main phone, 1, or two or more cordless handsets, preventing that raise secrecy nature and information is revealed outside.
[0002]
[Description of the Prior Art] Although the so-called wireless LAN (Local Area Network) is spreading in recent years, it is the so-called spread spectrum communication which is being generalized recently as one of the communication modulation techniques used for this wireless LAN. This spread spectrum communication is a communication mode which diffuses and transmits the energy of the signal which should be delivered and received to a latus frequency range rather than the original frequency which the signal has, and has the advantage of being able to stop power flux density low.
[0003] And since it is spreading as one method in this spread spectrum communication, it is a frequency-hopping method. Since the frequency to transmit changes every moment while it has the advantage which can stop power flux density lowest, when it is a method which transmits information and is considered in time sufficiently longer than the period of hopping, this method changing frequency with time, it has the advantage that resistance is high, also to disturbance or tapping.
[0004] It has the composition which delivers and receives information, holding the so-called hop table showing the changing frequency in common on both sides, and changing transmit frequencies and received frequency in a transmitting radio station and a receiving radio station according to this hop table, in order to synchronize the frequency which carries out hopping in the radio using the above-mentioned frequency-hopping method in the both sides of the transmitting radio station which transmits information, and the receiving radio station which receives information.
[0005] When extending no receiving tuning in to no transmitting tuning in at this time, in case the informational transfer which used the frequency-hopping method mutually is started, it is required in transmitting the above-mentioned hop table for no receiving tuning in from no transmitting tuning in, and starting informational transfer using the transmitted hop table concerned in no receiving tuning in beforehand.
[0006] It is common to start transmission of the information over the receiving radio station concerned, after having transmitted the so-called specific password to the transmitting radio station beforehand from the receiving radio station, acquiring the password concerned in the transmitting radio station, decoding this and, distinguishing that it is the above-mentioned specific receiving radio station on the other hand, when information is delivered and received for example, between the specific receiving radio stations and transmitting radio stations which were set up beforehand.
[0007]
[Problem(s) to be Solved by the Invention] However, when the hop table concerned was monitored during transmission of the above-mentioned hop table from the main phone before informational

transfer, a third person can acquire the hop table concerned and there was a trouble that there was a case where the secrecy nature of the information in a frequency-hopping method will fall remarkably, by this.

[0008] Moreover, when the password concerned is monitored in the transmission to the transmitting radio station of the above-mentioned password from a receiving radio station, a third person can acquire the password concerned and the secrecy nature of the information can receive now, and information should be delivered and received also in this case as a receiving radio station of specification [other radio stations other than the above-mentioned specific receiving radio station / **] will fall remarkably by this.

[0009] Although enciphering the information itself which should be delivered and received among the transmitting radio stations and receiving radio stations other than the above-mentioned hop table or a password that these troubles should be avoided is also considered In this case, if it is simple encryption in order to also complicate the circuitry for it and to reduction-ize an operation scale, while a large-scale operation is needed for informational encryption and an informational decryption, the trouble that secrecy nature will fall conversely will arise.

[0010] Then, this invention was made in view of each above-mentioned trouble, and the technical problem is in offering the radio method and the radio communications system which can raise the secrecy nature of the information between the transmitting radio station (henceforth a main phone) which is connected to external circuits, such as the telephone line, is fixed chiefly, and is used, and specification (henceforth a cordless handset), for example, a movable receiving radio station, which should be delivered and received.

[0011]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, invention according to claim 1 It is the radio method for performing it on radio, decoding transfer of the information between comrades, while secrecy-izing the information concerned using secrecy-ized information, such as a hop table. between a main phone and cordless handsets or the cordless handset concerned -- the information secrecy-ized [aforementioned] from the aforementioned main phone -- the above -- the above which does not have the secrecy-ized information concerned for the aforementioned secrecy-ized information for receiving in a cordless handset, and canceling and decoding the secrecy-ization concerned from the aforementioned main phone, when transmitting to a cordless handset In the cryptographic key information transmitting process transmitted from a cordless handset to the aforementioned main phone, and the aforementioned main phone the cryptographic key information for enciphering the secrecy-ized information concerned -- the above -- The encryption process which enciphers the aforementioned secrecy-ized information based on the cryptographic key information which carried out [aforementioned] reception, and generates enciphered secrecy-ized information, In a cordless handset the enciphered secrecy-ized information by which generation was carried out [aforementioned] -- the above from the aforementioned main phone -- the secrecy-ized information transmitting process transmitted to a cordless handset, and the above -- The enciphered secrecy-ized information by which transmission was carried out [aforementioned] is decoded using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and it has the restoration process which restores the aforementioned secrecy-ized information.

[0012] When transmitting secrecy-ized information in a cryptographic key information transmitting process to the cordless handset which does not have the secrecy-ized information concerned from a main phone according to the operation of invention according to claim 1, the cryptographic key information for enciphering the secrecy-ized information concerned is transmitted from a cordless handset to a main phone.

[0013] Next, in an encryption process, secrecy-ized information is enciphered based on the cryptographic key information received with the main phone, and enciphered secrecy-ized information is generated.

[0014] And in a secrecy-ized information transmitting process, the generated enciphered secrecy-ized information is transmitted to a cordless handset from a main phone.

[0015] Next, in a restoration process, the transmitted enciphered secrecy-ized information is decoded using the decode key information corresponding to cryptographic key information with a cordless handset, and secrecy-ized information is restored.
[0016] therefore -- since information is acquired canceling secrecy-ization using the secrecy-ized information which enciphered the secrecy-ized information for secrecy-izing the information itself which should be delivered and received, transmitted to the cordless handset from the main phone, and was restored in the cordless handset -- the case of only secrecy-izing of the information itself -- comparing -- a main phone and a cordless handset -- between or a cordless handset -- the secrecy nature of the information in transfer between comrades improves
[0017] Moreover, since the secrecy-ized information for transfer is enciphered and it transmits to the cordless handset concerned even when newly adding the cordless handset which does not have secrecy-ized information beforehand and starting informational transfer, secrecy-ized information is not revealed outside and the secrecy nature in informational transfer improves.
[0018] In order to solve the above-mentioned technical problem, invention according to claim 2 a setup to which the cordless handset concerned between a main phone and a cordless handset was beforehand set in the main phone concerned, while performing transfer of identification information, such as a password for discriminating whether it is a cordless handset, on radio, secrecy-izing the identification information concerned In a cordless handset the aforementioned main phone and the aforementioned setup -- the cryptographic key information for being the radio method for delivering and receiving the information between cordless handsets on radio, and enciphering the aforementioned identification information -- the above from the aforementioned main phone -- the cryptographic key information transmitting process transmitted to a cordless handset, and the above -- In the identification information transmitting process transmitted to the aforementioned main phone from a cordless handset, and the aforementioned main phone the encryption process which enciphers the aforementioned identification information based on the cryptographic key information which carried out [aforementioned] reception, and generates encryption identification information, and the encryption identification information by which generation was carried out [aforementioned] -- the above -- In the restoration process which decodes the encryption identification information by which transmission was carried out [aforementioned] using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and restores the aforementioned identification information, and the aforementioned main phone the above which transmitted the aforementioned encryption identification information based on the identification information by which restoration was carried out [aforementioned] -- a cordless handset -- the aforementioned setup -- the judgment process which judges whether it is a cordless handset, and the above which transmitted the aforementioned encryption identification information -- a cordless handset -- the aforementioned setup, when it is distinguished that it is a cordless handset the setup concerned from the aforementioned main phone -- it has the transmitting process which transmits the aforementioned information to a cordless handset
[0019] According to the operation of invention according to claim 2, in a cryptographic key information transmitting process, cryptographic key information is transmitted from a main phone to a cordless handset.
[0020] And in an encryption process, based on the received cryptographic key information, identification information is enciphered with a cordless handset, and encryption identification information is generated.
[0021] Next, in an identification information transmitting process, the generated encryption identification information is transmitted to a main phone from a cordless handset.
[0022] Then, in a restoration process, the transmitted encryption identification information is decoded with a main phone using decode key information, and identification information is restored.
[0023] and the cordless handset which transmitted encryption identification information in the judgment process based on the restored identification information -- a setup -- it judges with a main phone whether it is a cordless handset
[0024] the cordless handset which finally transmitted encryption identification information in the

transmitting process -- a setup -- the time of it being distinguished that it is a cordless handset -- the setup concerned from a main phone -- information is transmitted to a cordless handset
[0025] therefore -- although learning of the identification information is carried out outside -- things -- there is nothing -- certain -- a setup -- a cordless handset can be discriminated, and information can be delivered and received
[0026] In order to solve the above-mentioned technical problem, invention according to claim 3 It is the radio communications system which performs it on radio, decoding transfer of the information between comrades while secrecy-izing the information concerned using secrecy-ized information, such as a hop table. between a main phone and cordless handsets or the cordless handset concerned -- the above -- the information which is the cryptographic key information transmitting means included in a cordless handset, and was secrecy-ized [aforementioned] from the aforementioned main phone -- the above -- the aforementioned secrecy-ized information for receiving in a cordless handset, and canceling and decoding the secrecy-ization concerned the above which does not have the secrecy-ized information concerned from the aforementioned main phone, while being contained in a cryptographic key information transmitting means and the aforementioned main phones, such as the transceiver section which transmits the cryptographic key information for enciphering the secrecy-ized information concerned to the aforementioned main phone, when transmitting to a cordless handset While being contained in an encryption means and the aforementioned main phones, such as a code machine which enciphers the aforementioned secrecy-ized information based on the cryptographic key information which carried out [aforementioned] reception, and generates enciphered secrecy-ized information the enciphered secrecy-ized information by which generation was carried out [aforementioned] -- the above -- secrecy-ized information transmitting meanses, such as the transceiver section which transmits to a cordless handset, and the above, while being contained in a cordless handset The enciphered secrecy-ized information by which transmission was carried out [aforementioned] is decoded using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and it has restoration meanses, such as a decoder which restores the aforementioned secrecy-ized information.
[0027] According to the operation of invention according to claim 3, the cryptographic key information transmitting means included in a cordless handset transmits the cryptographic key information for enciphering the secrecy-ized information concerned to a main phone, when transmitting secrecy-ized information from a main phone to the cordless handset which does not have the secrecy-ized information concerned.
[0028] And the encryption means included in a main phone enciphers secrecy-ized information based on the received cryptographic key information, and generates enciphered secrecy-ized information.
[0029] Then, the secrecy-ized information transmitting means included in a main phone transmits the generated enciphered secrecy-ized information to a cordless handset.
[0030] Finally, the restoration means included in a cordless handset decodes the transmitted enciphered secrecy-ized information using decode key information, and restores secrecy-ized information.
[0031] therefore -- since information is acquired canceling secrecy-ization using the secrecy-ized information which enciphered the secrecy-ized information for secrecy-izing the information itself which should be delivered and received, transmitted to the cordless handset from the main phone, and was restored in the cordless handset -- the case of only secrecy-izing of the information itself -- comparing -- a main phone and a cordless handset -- between or a cordless handset -- the secrecy nature of the information in transfer between comrades improves
[0032] Moreover, since the secrecy-ized information for transfer is enciphered and it transmits to the cordless handset concerned even when newly adding the cordless handset which does not have secrecy-ized information beforehand and starting informational transfer, secrecy-ized information is not revealed outside and the secrecy nature in informational transfer improves.
 [0033] In order to solve the above-mentioned technical problem, while invention according to claim 4 changes in time the frequency used for transfer of the information concerned and secrecy-ization of the aforementioned information is performed for it in a radio communications system according to claim 3, the aforementioned secrecy-

ized information is constituted so that it may be the table information referred to when changing the aforementioned frequency.
[0034] While according to the operation of invention according to claim 4 in addition to an operation of invention according to claim 3 informational secrecy-ization changes in time the frequency used for transfer of the information concerned and is performed Since it is the table information referred to when secrecy-ized information changes frequency, information can be kept secret still more effectively to tapping etc. by secrecy-izing transfer of table information and performing it.
[0035] In order to solve the above-mentioned technical problem, while being a public key [in / a public key cryptosystem / on a radio communications system according to claim 3 or 4 and / invention / according to claim 5 / in the aforementioned cryptographic key information], the aforementioned decode key information is constituted so that it may be a private key in the aforementioned public key cryptosystem.
[0036] According to the operation of invention according to claim 5, in addition to an operation of invention according to claim 3 or 4, since decode key information is a private key in a public key cryptosystem while cryptographic key information is a public key in a public key cryptosystem, informational secrecy nature can be raised further.
[0037] in order to solve the above-mentioned technical problem, while invention according to claim 6 is creation information, such as initial value for the aforementioned secrecy-ized information generating the table information referred to when changing the aforementioned frequency, in a radio communications system according to claim 4 or 5 -- the above -- a cordless handset is further equipped with generation meanses, such as a hop table generation machine for generating the aforementioned table information using the creation information concerned
[0038] While being the creation information for generating the table information referred to when secrecy-ized information changes frequency in addition to an operation of invention according to claim 4 or 5 according to the operation of invention according to claim 6, it has further a generation means for a cordless handset generating table information using the creation information concerned.
[0039] Therefore, the information which acquired table information and has been more quickly transmitted in a cordless handset as compared with the case where encipher the table information itself as secrecy-ized information, and it transmits to a cordless handset from a main phone can be decoded.
[0040] In order to solve the above-mentioned technical problem, invention according to claim 7 a setup to which the cordless handset concerned between a main phone and a cordless handset was beforehand set in the main phone concerned, while performing transfer of identification information, such as a password for discriminating whether it is a cordless handset, on radio, secrecy-izing the identification information concerned It is a radio communications system for delivering and receiving the information between cordless handsets on radio. the aforementioned main phone and the aforementioned setup -- the cryptographic key information for being the cryptographic key information transmitting means included in the aforementioned main phone, and enciphering the aforementioned identification information -- the above -- cryptographic key information transmitting meanses, such as the transceiver section which transmits to a cordless handset, and the above, while being contained in a cordless handset encryption meanses, such as a code machine which enciphers the aforementioned identification information based on the cryptographic key information which carried out [aforementioned] reception, and generates encryption identification information, and the above, while being contained in a cordless handset While being contained in an identification information transmitting means and the aforementioned main phones, such as the transceiver section which transmits the encryption identification information by which generation was carried out [aforementioned] to the aforementioned main phone While being contained in a restoration means and the aforementioned main phones, such as a decoder which decodes the encryption identification information by which transmission was carried out [aforementioned] using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and restores the aforementioned identification information the above which transmitted the aforementioned encryption identification information based on the identification information by which restoration was carried out [aforementioned] -- a cordless handset -- the

aforementioned setup, while being contained in a judgment means and the aforementioned main phones, such as a controller which judges whether it is a cordless handset the above which transmitted the aforementioned encryption identification information -- a cordless handset -- the aforementioned setup -- the time of it being distinguished that it is a cordless handset -- the setup concerned -- it has transmitting meanses, such as the transceiver section which transmits the aforementioned information to a cordless handset

[0041] According to the operation of invention according to claim 7, the cryptographic key information transmitting means included in a main phone transmits cryptographic key information to a cordless handset.

[0042] And the encryption means included in a cordless handset enciphers identification information based on the received cryptographic key information, and generates encryption identification information.

[0043] Then, the identification information transmitting means included in a cordless handset transmits the generated encryption identification information to a main phone.

[0044] Next, the restoration means included in a main phone decodes the transmitted encryption identification information using decode key information, and restores identification information.

[0045] and the cordless handset which transmitted encryption identification information based on the identification information to which the judgment means included in a main phone was restored -- a setup -- it judges whether it is a cordless handset

[0046] the cordless handset with which the transmitting means included in a main phone finally transmitted encryption identification information -- a setup -- the time of it being distinguished that it is a cordless handset -- the setup concerned -- information is transmitted to a cordless handset

[0047] therefore, the thing done outside for learning of the identification information -- there is nothing -- certain -- a setup -- a cordless handset can be discriminated, and information can be delivered and received

[0048] In order to solve the above-mentioned technical problem, while being a public key [in / a public key cryptosystem / on a radio communications system according to claim 7 and / invention / according to claim 8 / in the aforementioned cryptographic key information], the aforementioned decode key information is constituted so that it may be a private key in the aforementioned public key cryptosystem.

[0049] According to the operation of invention according to claim 8, in addition to an operation of invention according to claim 7, since decode key information is a private key in a public key cryptosystem while cryptographic key information is a public key in a public key cryptosystem, informational secrecy nature can be raised further.

[0050]

[Embodiments of the Invention] Next, the gestalt of the suitable operation for this invention is explained using a drawing.

[0051] (I) The 1st operation gestalt concerning this invention is explained at the beginning of the 1st operation gestalt using drawing 1 or drawing 5 . Here, while the 1st operation gestalt explained below is beforehand formed with a main phone, 1, or two or more cordless handsets, when newly adding a cordless handset and starting informational transfer with the frequency-hopping method concerned to the radio communications system using the frequency-hopping method, it is a gestalt of the operation which applied this invention.

[0052] First, the whole main phone composition and outline operation which constitute the radio communications system of this operation gestalt are explained using drawing 1 .

[0053] As shown in drawing 1 , this soma 10 which processes the information received while the main phone SO generated the information which should be transmitted, and the information transmitted from the cordless handset while transmitting the information which should be transmitted to a cordless handset through Antenna ANT are received through the antenna ANT concerned, and it is constituted by the transceiver section 1 as a secrecy-ized information transmitting means output to this soma 10.

[0054] And the transceiver section 1 is constituted by an interface 2, the strange recovery section 3, an

up converter 4, power amplification 5, the transmission-and-reception circuit changing switch 6, the low noise amplifier 7, the down converter 8, and PLL (Phase Locked Loop)9 and the above-mentioned antenna ANT.
[0055] Moreover, RAM11 which memorizes temporarily the information which should deliver and receive this soma 10 between cordless handsets (Random Access Memory), Hop table storing section 11A which memorizes the information which it has in RAM11 concerned and is included in a hop table, The code machine 12 as an encryption means to encipher a hop table in the below-mentioned processing, It is constituted by the circuit changing switch 13 which changes the information which should carry out the above-mentioned transfer with the output of the code machine 12, and is outputted to the transceiver section 1, the controller 14 which controls the whole main phone SO, and the power supply section 15 which supplies supply voltage through a controller 14 to each composition member of a main phone SO.
[0056] Next, the whole cordless handset composition and outline operation which constitute the radio communications system of this operation form are explained using drawing 2 .
[0057] it is shown in drawing 2 -- as -- a cordless handset -- an SC is constituted by the transceiver section 20 as this soma 30 which processes the information received while generating the information which should be transmitted, and a cryptographic key information transmitting means receive through the antenna ANT concerned and output the information transmitted from the main phone SO to this soma 30 while transmitting the information which should be transmitted to a main phone SO through Antenna ANT
[0058] And the transceiver section 20 is constituted by an interface 21, the strange recovery section 22, an up converter 23, power amplification 24, the transmission-and-reception circuit changing switch 25, the low noise amplifier 26, the down converter 27, and PLL (Phase Locked Loop)28 and the above-mentioned antenna ANT.
[0059] Moreover, RAM31 which memorizes temporarily the information which should deliver and receive this soma 30 between main phones, Hop table storing section 31A which memorizes the information which it has in RAM31 concerned and is included in a hop table, The decoder 32 as a restoration means to restore the hop table transmitted in the below-mentioned processing, the circuit changing switch 33 which changes the information which should carry out the above-mentioned transfer with the output of a decoder 32, and is outputted to the transceiver section 20, and a cordless handset -- the controller 34 which controls the whole SC, and a controller 34 -- minding -- a cordless handset -- it is constituted by the power supply section 35 which supplies supply voltage to each composition member of SC
[0060] next, a main phone SO and a cordless handset -- details operation of SC is explained using drawing 1 or drawing 5
[0061] Operation of transfer (a hop table a main phone SO and a cordless handset transfer of the information which is acquired in SC and performed by the frequency-hopping method based on this) of the general information in the radio communications system of introduction and this operation gestalt is explained using drawing 1 or drawing 3 .
[0062] first, a main phone SO to information -- transmitting -- a cordless handset -- the processing in the case of receiving this in SC is explained
[0063] the cordless handset from a main phone SO -- when transmitting information to SC, it is shown in drawing 1 -- as -- an information signal Sif -- a cordless handset, in case it transmits to SC The information on the above-mentioned hop table stored in hop table storing section 11A in RAM11 is outputted to PLL9 as a table signal Stt, and it sets to PLL9 concerned. While generating the local signal Sc of the frequency set as the hop table concerned with reference to the table signal Stt based on the control signal Spl from a controller 14, a frequency lock is carried out and it outputs to the above-mentioned up converter 4. On the other hand, once the information concerned which should be transmitted is stored in RAM11, it is outputted to a circuit changing switch 13 as an information signal Sif. At this time, the circuit changing switch 13 concerned is changed to the information signal Sif side based on the control signal Ssw1 from a controller 14.

[0064] And if the information signal Sif concerned is outputted to the transceiver section 1 through a circuit changing switch 13, with an interface 2, corresponding to the attribute of an information signal Sif, incorporation operation (interface operation) to the transceiver section 1 is performed, and a predetermined modulation will be given in a modulator and demodulator 3, and it will be outputted as a modulating signal Smi, and will be outputted to an up converter 4.
[0065] In the up converter 4 constituted by the mixer etc., the frequency of the above-mentioned modulating signal Smi and the frequency of the local signal Sc are added by these, and it is outputted to power amplification 5 as a sending signal St, and is amplified by the predetermined amplification factor. then, the sending signal St concerned -- the transmission-and-reception circuit changing switch 6 (based on the control signal Ssw2 from a controller 14, it changes to the sending-signal St side.) -- minding -- the cordless handset from Antenna ANT -- it is transmitted to SC Corresponding to time, it will change with operation of this up converter 4 so that the frequency when transmitting a sending signal St may contain the frequency set up as a hop table.
[0066] Next, reception operation in a cordless handset is explained using drawing 2 .
[0067] the information containing the sending signal St transmitted changing frequency from a main phone SO -- a cordless handset -- it is received in the antenna ANT in SC, and is amplified by the predetermined amplification factor in the low noise amplifier 26 through the transmission-and-reception circuit changing switch 25 as an input signal Sr At this time, the transmission-and-reception circuit changing switch 25 is changed to the low noise amplifier 26 side based on the control signal Ssw2 from a controller 34. And the input signal Sr amplified with low noise amplifier is outputted to a down converter 27.
[0068] on the other hand -- the information from a main phone SO -- a cordless handset, in case it receives in SC The above-mentioned hop table stored in hop table storing section 31A in RAM31 (it has the same contents as the hop table of a main phone SO.) Information is outputted to PLL28 as a table signal Stt, and it sets to PLL28 concerned. The local signal Sc of the frequency set as the hop table concerned with reference to the table signal Stt based on the control signal Spl from a controller 34 is outputted to the above-mentioned down converter 27.
[0069] In the down converter 27 constituted by the mixer etc., the frequency of the local signal Sc is subtracted from the frequency of the above-mentioned input signal Sr, it becomes the modulating signal Smi in a main phone SO, and the recovery signal Sni which is same signal, and is outputted to a modulator and demodulator 22, and recovery operation is performed in the modulator and demodulator 22 concerned by these, and it is outputted to this soma 30 through an interface 21.
[0070] Then, the signal to which it restored is outputted as an information signal Sif through a circuit changing switch 33 in this soma 30, and is temporarily memorized by RAM31. At this time, the circuit changing switch 33 is changed to the information signal Sif side based on the control signal Ssw1 from a controller 34.
[0071] After that, predetermined processing etc. is performed to the memorized information by the processing section which is not illustrated.
[0072] the main phone [in / this operation form / here] SO, and a cordless handset -- the structure of the information transmitted and received between SCs is explained using drawing 3
[0073] In the radio communications system of this operation form, two-way communication is performed using the so-called TDD (time-sharing dupe REKUSU) method. namely, the cordless handset from for example, the main phone SO -- in transmitting information to SC, as shown in drawing 3 (a), by making into a unit the frame 16 which consists of frequency hop phase block 16A, transmitting phase block 16B, transmission-and-reception change phase block 16C, and receiving phase block 16D, a main phone SO constitutes information and operates on the other hand -- a cordless handset -- as shown in drawing 3 (a), by making into a unit the frame 17 which consists of frequency hop phase block 17A, receiving phase block 17B, transmission-and-reception change phase block 17C, and transmitting phase block 17D, SC constitutes information and operates At this time, the timing from a start within each frame to an end is set up beforehand, and these the phase blocks of each are managed. Moreover, the hopping (change) of frequency is performed for every frame, and when having transmitted and received

the information which constitutes the frame of 1, frequency does not change.
[0074] the period which stabilizes the transceiver frequency from which the frequency hop phase blocks 16A and 17A will be in a transition state with the change of a frame among these phase blocks -- it is -- a main phone SO or a cordless handset -- informational transmission and reception are not performed between SCs
[0075] moreover, in transmitting phase block 16B (namely, a cordless handset receiving phase block 17B of SC) of a main phone SO the cordless handset from a main phone SO -- to the information concerned in the period when information is transmitted to SC everything but the above-mentioned sending signal St -- as a control signal -- a main phone SO and a cordless handset -- the synchronizing signal for taking the synchronization with SC for every frame -- a cordless handset -- the call signal for calling SC, and a cordless handset -- the busy signal which shows the purport with which the connection enabling signal and main phone SO in which the purport that the call concerned from SC was received is shown are communicating is contained
[0076] furthermore, transmission-and-reception change phase block 16C or 17C -- a main phone SO and a cordless handset -- between the transient phases with which SC is alike, respectively and it sets and which transmission and reception replace -- a main phone SO or a cordless handset -- informational transmission and reception are not performed between SCs
[0077] At the end, receiving phase block 16D (namely, a cordless handset transmitting phase block 17D of SC) of a main phone SO the below-mentioned operation -- a cordless handset -- to the information concerned in the period when information is transmitted to a main phone SO from SC the below-mentioned cordless handset -- everything but the sending signal St in SC -- as a control signal -- a cordless handset -- the synchronous acknowledge signal which answers that the synchronization with a main phone SO was able to be taken by the SC side -- the connection consent signal and cordless handset in which the call signal which calls a main phone SO, and the purport that the call was received from the main phone SO are shown -- the busy signal which shows the purport with which SC is communicating is contained
[0078] in one frame, transmission and reception are performed by making into a unit the frame constituted by each above-mentioned phase block, and the transmission and reception concerned are repeatedly performed over two or more frames -- a main phone SO and a cordless handset -- communication bidirectional in between SCs will be performed moreover, each above-mentioned frame -- a main phone SO and a cordless handset -- it is constituted based on the control signal Sm from each controller in SC
[0079] next, a cordless handset -- information is transmitted from SC and the processing in the case of receiving this in a main phone SO is explained
[0080] a cordless handset -- operation in the case of transmitting information from SC to a main phone SO -- fundamental -- the cordless handset from the above-mentioned main phone SO -- the main phone SO in operation in the case of transmitting information to SC, and a cordless handset -- it is equivalent the processing at the time of replacing SC
[0081] namely, a cordless handset -- the information memorized by RAM11 of SC is outputted to an up converter 23 as a modulating signal Smi through a circuit changing switch 33, an interface 21, and a modulator and demodulator 22 as an information signal Sif And in the up converter 23 concerned, the frequency of the local signal Sc corresponding to the frequency information in the hop table from PLL28 is added, and it is amplified in power amplification 24, and is transmitted from Antenna ANT through the transmission-and-reception circuit changing switch 25. At this time, the frequency for transmission and reception will change for every above-mentioned frame.
[0082] And the signal received in the antenna ANT of a main phone SO In the low noise amplifier 7, it is amplified through the transmission-and-reception circuit changing switch 6 as an input signal Sr. In a down converter 8, the frequency of the local signal Sc is subtracted from the frequency of the input signal Sr concerned, and it becomes the recovery signal Sni. This is sent to this soma 10 through the post-interface 2 to which it restored in the modulator and demodulator 3, and is temporarily stored in RAM11 through a circuit changing switch 13.

[0083] operation of each part explained above -- a frequency-hopping method -- using -- a main phone SO and a cordless handset -- informational two-way communication will be performed between SCs
[0084] Next, it explains, illustrating about the hop table used for the frequency-hopping method concerned using drawing 3 (b). In addition, drawing 3 (b) shows the state where four kinds of tables (the tables f and k which contain N kinds of frequency, respectively) are memorized as a hop table by hop table storing section 11A in a main phone SO.
[0085] this time, for example, N kinds of frequency indicated by Table f, -- the cordless handset from the main phone SO of call control or the below-mentioned hop table itself -- the information which should keep secret N kinds of frequency which is used for the frequency change at the time of transmitting to SC, and is indicated by Tables g and k, respectively -- the cordless handset from a main phone SO -- it is used for the frequency change at the time (at the time of information communication) of actually transmitting to SC the frequency contained in the table of 1 at this time -- the cordless handset of 1 -- it is used for communication between SCs that is, -- the case where it is shown in drawing 3 (b) -- the main phone SO of 1 -- receiving -- three sets of cordless handsets -- SC -- radio connection -- carrying out -- the cordless handset of 1 -- it becomes possible to assign the table of one among Tables g and k to SC, and to transmit and receive information
[0086] next, the main phone SO concerning this invention -- new -- a cordless handset -- the above-mentioned hop table at the time of making radio connection of the SC -- the cordless handset from a main phone SO -- the processing for transmitting to SC is explained using the flow chart shown in drawing 1 , drawing 2 , drawing 4 , and drawing 5 in addition, the flow chart which the flow chart shown in drawing 4 shows the processing in a main phone SO, and is shown in drawing 5 -- a cordless handset -- the processing in SC is shown and a controller 14 or the processing in 34 is mainly shown
[0087] Operation in introduction and a main phone SO is explained using drawing 1 and drawing 4 .
[0088] a new cordless handset, in case the hop table for information communication (for example, any one hop table in the tables g and k in drawing 3 (b)) is transmitted from a main phone SO to SC It is judged whether there was any call from SC (Step S2). introduction and the main phone SO which is carrying out reception standby (Step S1) -- setting -- the cordless handset concerned which should be connected newly -- the case (Step S2; YES) where there is a call -- the cordless handset concerned -- ID information (the cordless handset of 1 -- it is the information for specifying SC and is the information included at the head for every ** frame) from SC Usually this ID information is transmitted and received, without being enciphered. It receives (Step S3). and received ID information -- the cordless handset concerned -- the cordless handset with which SC is registered beforehand -- it judges whether it is ID information on SC (the cordless handset (it may connect in the future) which can connect ID information to a main phone SO -- beforehand registered as ID information on SC) (Step S4)
[0089] It is judged whether the predetermined time set up beforehand (Step S2; NO) from SC when there was no call passed (Step S6). on the other hand -- the judgment of Step S2 -- setting -- a cordless handset -- When having not passed, a reception (Step S6; NO) standby state (Step S1) is continued, and when having passed, a main phone (Step S6; YES) SO is made into a sleep state (Step S15).
[0090] moreover, the cordless handset registered in the judgment of Step S4 -- the time of not being SC - (Step S4; NO) and the cordless handset which had planned connection beforehand -- ****** it is not SC -- the cordless handset concerned -- it returns to Step S1 that communication with SC should be made into ** (Step S5), and reception standby should be carried out as it is
[0091] The public key signal Sko transmitted from SC is received like the usual information in the transceiver section 1 (Step S7). furthermore, the cordless handset registered in the judgment of Step S4 -- the time of being SC -- a degree (Step S4; YES) -- the cordless handset concerned -- The public key information included in the received public key signal Sko concerned is used. The table signal Stt corresponding to the hop table of any 1 of the hop tables for information communication memorized by hop table storing section 11A (the cordless handset which it is going to connect hop table which should be used for radio with SC) is enciphered in the code machine 12. The encryption table signal Sta is outputted (Step S8). then, the encryption table signal Sta concerned -- the transceiver section 1 -- minding -- a cordless handset -- it transmits to SC (Step S9) At this time, the circuit changing switch 13

has changed to the code machine 12 side. moreover, the encryption table signal Sta -- a cordless handset -- it is transmitted to frequency hopping at the time of transmitting to SC, frequency being changed using the table f (this table -- all cordless handsets -- SC has beforehand) shown in drawing 3 (b) Furthermore, in the encryption in Step S8, cipher systems, such as a RSA (Rivest-Shamir-Adleman) code in a public key cryptosystem, an ElGamal code, a elliptic curve cryptosystem, an ellipse RSA code, or an inverse number code, are used, and encryption is performed, for example.

[0092] the cordless handset which the above-mentioned public key is used in the so-called public key cryptosystem, and should acquire the hop table for radio in this operation form here -- the main phone SO with which SC transmitted the public key signal Sko corresponding to a public key to the main phone SO, and received this -- setting -- the public key concerned -- using -- the hop table for radio -- enciphering -- the enciphered hop table concerned -- a cordless handset -- it transmits to SC and the cordless handset which received this -- in SC, a code will be decoded using the private key (it differs from the public key itself.) corresponding to the above-mentioned public key, and a hop table will be acquired

[0093] It checks from SC whether there is any resending demand of the below-mentioned encryption table signal Sta (Step S10). if the encryption table signal Sta is transmitted -- next, a cordless handset -- When there is a resending demand (Step S10; YES), it resends (Step S9). the time of there being no resending demand -- (Step S10; NO) and a degree -- a cordless handset -- it stands by until it checks whether the below-mentioned completion signal of reception of SC has been received (Step S11), and it receives (Step S11; NO), when having not received

[0094] the cordless handset (Step S9) which changed from (Step S11; YES) and the table f which was using the hop table for the degree till then to the hop table for radio (hop (Step S9) table enciphered and transmitted) on the other hand when the completion signal of reception was received (Step S12), and transmitted the hop table for the radio concerned -- the concrete communication by the frequency-hopping method starts between SCs (Step S13)

[0095] And when it is judged whether communication was completed or not (Step S14) and it is not completed, communication is continued as it is (Step S14; NO) (Step S13), and when having ended, it shifts to (Step S14; YES) and a sleep state (Step S15). And when it is judged whether the power supply of a main phone SO was made into ** (Step S16) and it is made into ** (Step S16; YES), processing is ended as it is, and when not considering as **, a sleep (Step S16; NO) state is continued (Step S15).

[0096] next, the cordless handset corresponding to operation of the above-mentioned main phone SO -- hop table acquisition operation of SC is explained using drawing 2 and drawing 5

[0097] In SC the cordless handset which should newly be connected corresponding to operation of the above-mentioned main phone SO -- Introduction, The above-mentioned ID information () [<A HREF="/Tokujitu/tjitemdrw.ipdl?N0000=239&N0500=1E_N/;> ? ==;<;?///&N0001=730&N0552=9&N0553=000006"] TARGET="tjitemdrw"> drawing 4 step S3 reference -- transmitting (Step S20) -- next, a cordless handset -- the above-mentioned public key signal Sko corresponding to the public key beforehand stored in RAM11 of SC is transmitted to a main phone SO through the transceiver section 20 (Step S21) In transmission of this public key signal Sko, frequency hopping which used the above-mentioned table f is performed.

[0098] Next, the above-mentioned (refer to drawing 4 step S9) encryption table signal Sta transmitted from the main phone SO corresponding to the transmitted public key signal Sko is received (Step S22). And when it is judged whether it was receivable errorless (Step S23) and it is not able to receive, a resending demand is performed to a main phone (Step S23; YES) SO (Step S24.). The encryption table signal Sta resent to the drawing 4 step S10 reference step S22 by returning is received.

[0099] On the other hand, when the encryption table signal Sta is able to be received errorless, the received encryption table signal Sta is restored as an original hop table in a decoder 32 using the private key signal Ssc corresponding to the above-mentioned private key stored in (Step S23; NO), next RAM31 (Step S25). And the above-mentioned completion signal which shows that reception of the encryption table signal Sta was completed is transmitted to a main phone SO (Step S26.). It changes to the hop table for radio which restored the hop table to drawing 4 step S11 reference and the degree from

the table f which was being used till then (Step S27), and the concrete communication by the frequency-hopping method is started between the main phones SO concerned (Step S28).
[0100] And when it is judged whether communication was completed or not (Step S29) and it is not completed, communication is continued as it is (Step S29; NO) (Step S28), and when having ended, it shifts to (Step S29; YES) and a sleep state (Step S30). and a cordless handset -- when it is judged whether the power supply of SC was made into ** (Step S31) and it is made into ** (Step S31; YES), processing is ended as it is, and when not considering as **, a sleep (Step S31; NO) state is continued (Step S30)
[0101] the hop table for secrecy-izing the information itself which should be delivered and received according to operation of the radio communications system of the 1st operation gestalt explained above -- enciphering -- the cordless handset from a main phone SO -- an SC -- transmitting -- a cordless handset -- the case of only secrecy-izing of the information by the frequency-hopping method itself since information receives using the hop table restored in SC -- comparing -- a main phone SO and a cordless handset -- the secrecy nature of the information in transfer between SCs improves
[0102] moreover, the cordless handset which does not have a hop table beforehand -- the case where newly add SC and informational transfer is started -- the hop table for transfer -- enciphering -- the cordless handset concerned -- since it transmits to SC, a hop table is not revealed outside and the secrecy nature in informational transfer improves
[0103] Furthermore, information can be kept secret still more effectively to tapping etc. by secrecy-izing transfer of the hop table in a frequency-hopping method, and performing it.
[0104] Moreover, since a hop table is transmitted using a public key cryptosystem, informational secrecy nature can be raised further.
[0105] in addition, the direction of a **** -- a cordless handset -- if SC acquires a hop table, since the hop table concerned will not be revealed outside -- two or more cordless handsets -- the case where SC is connected to the main phone -- the cordless handset concerned -- the secrecy nature of transfer of the information between SCs will also improve
[0106] Moreover, although considered as the composition which acquires the public key signal Sko and the encryption table signal Sta through each interface, you may make it deliver and receive through each controller in the above-mentioned operation gestalt not only this but directly.
[0107] (II) The 2nd operation gestalt which is the 2nd operation gestalt, next other operation gestalten concerning this invention is explained using drawing 6 and drawing 7 . the cordless handset which drawing 6 is drawing showing the composition of main phone SO' concerning the 2nd operation gestalt here, and drawing 7 requires for the 2nd operation gestalt -- it is drawing showing the composition of SC'
[0108] the above-mentioned 1st operation gestalt -- setting -- a cordless handset -- the public key from SC -- using -- a main phone SO -- setting -- the hop table itself -- enciphering -- this -- a cordless handset, although it transmits to SC, it restores to it and the hop table was acquired the initial value for generating a hop table in the 2nd operation gestalt -- a cordless handset -- the public key from SC -- using -- a main phone SO -- setting -- enciphering -- a cordless handset -- SC -- transmitting -- the cordless handset concerned -- a hop table is generated using the initial value enciphered in SC
[0109] in addition, drawing 6 and drawing 7 -- setting -- the member same about the respectively same composition member as drawing 1 and drawing 2 -- a number is attached and explanation of details is omitted
[0110] The composition of main phone SO' concerning introduction and the 2nd operation gestalt is explained using drawing 6 .
[0111] As shown in drawing 6 , while having RAM40 equipped with initial value storing section 40A which stores the initial value used in case main phone SO' concerning the 2nd operation gestalt is replaced with RAM11 in the 1st operation gestalt and a hop table is generated, it has the hop table generation machine 41 which generates the hop table for radio using the initial value concerned. Other composition is the same as that of the above-mentioned main phone SO.
[0112] next, the cordless handset concerning the 2nd operation gestalt -- the composition of SC' is

explained using drawing 7
[0113] the cordless handset applied to the 2nd operation gestalt as shown in drawing 7 -- SC' was replaced with RAM31 in the 1st operation gestalt, and it is equipped with the hop table generation machine 51 as a generation means to generate the hop table for radio using the initial value concerned while it is equipped with RAM50 equipped with initial value storing section 50A which stores the above-mentioned initial value other composition -- the above -- a cordless handset -- it is the same as that of SC
[0114] next, main phone SO' which has the above composition and a cordless handset -- operation of the 2nd operation gestalt in the radio communications system constituted by SC' is explained
[0115] the 2nd operation gestalt -- setting -- a new cordless handset -- the time of connecting SC' -- introduction -- this -- this -- the public key signal Sko corresponding to the above-mentioned public key is transmitted to cordless handset SC' to main phone SO'
[0116] and the initial value signal Si corresponding to the initial value (the cordless handset which it is going to connect initial value for generating the hop table which should be used for radio with SC') beforehand stored in main phone SO' which received this using the public key concerned -- the code machine 12 -- setting -- enciphering -- the encryption initial value signal Sia -- outputting -- the encryption initial value signal Sia concerned -- the transceiver section 1 -- minding -- a cordless handset -- it transmits to SC'
[0117] the cordless handset which, on the other hand, received the encryption initial value signal Sia -- in SC', the encryption initial value signal Sia concerned is acquired by this soma 30' through the transceiver section 20, this is restored in a decoder 32 using the above-mentioned private key signal Ssc, the original initial value signal Si is generated, and it stores in initial value storing section 50A in RAM50
[0118] Next, in main phone SO', in the hop table generation machine 41, a hop table is generated using the initial value stored beforehand, and information is delivered [outputting the corresponding table signal Stt to PLL9, and performing frequency hopping] in the case of transmission of the information which should originally be delivered and received and received.
[0119] on the other hand -- a cordless handset -- in SC', the initial value transmitted and restored from main phone SO' is taken out from initial value storing section 50A, a hop table is generated in the hop table generation machine 51, and information is delivered and received, outputting the corresponding table signal Stt to PLL28, and performing frequency hopping
[0120] the case where according to operation of the radio communications system of the 2nd operation gestalt explained above encipher only initial value and transmit, and encipher the hop table itself and it transmits to a cordless handset from a main phone by [which received this] decoding -- comparing -- more -- quick -- a cordless handset -- the information which acquired the hop table and has been transmitted in SC' can be decoded
[0121] In addition, when a controller 14 or 34 functions using software, you may make it achieve the function of the hop table generation machines 41 and 51 concerned about the above-mentioned hop table generation machines 41 and 51. Moreover, it is also assignable using the shift register which has a predetermined feedback tap.
[0122] (III) The 3rd operation gestalt which is the 3rd operation gestalt, next other operation gestalten concerning this invention is explained using drawing 8 or drawing 11 . the cordless handset which drawing 8 is drawing showing the composition of main phone SO" concerning the 3rd operation gestalt here, and drawing 9 requires for the 3rd operation gestalt -- it is drawing showing the composition of SC" moreover, a cordless handset [in / the 3rd operation gestalt / drawing 10 is a flow chart which shows operation of main phone SO" in the 3rd operation gestalt, and / in drawing 11] -- it is the flow chart which shows operation of SC"
[0123] the [above / the 1st or] -- in 2 operation gestalten, although the operation gestalt of the radio communications system which secrecy-izes acquisition of the hop table for a frequency-hopping method was explained, a **** 3 operation gestalt is an operation gestalt about the radio communications system for secrecy-izing the so-called transfer of the password for judging whether the cordless handset which

is going to be connected to main phone SO" is cordless handset SC" by which setting registration is carried out beforehand
[0124] in addition, drawing 6 and drawing 7 -- setting -- the member same about the respectively same composition member as drawing 1 and drawing 2 -- a number is attached and explanation of details is omitted
[0125] The composition of main phone SO" concerning introduction and the 3rd operation gestalt is explained using drawing 8 .
[0126] As shown in drawing 8 , main phone SO" concerning the 3rd operation gestalt While replacing with this soma 10 in the 1st operation gestalt and memorizing temporarily the information which should be delivered and received a password -- storing -- a password -- storing -- the section -- 60 -- A -- having had -- RAM -- 60 -- the after-mentioned -- encryption -- a password -- a signal -- Stw -- being based -- a password -- restoring -- a decoder -- 61 -- judgment -- a means -- ****** -- a **** -- a controller -- 14 -- and -- a power supply section -- 15 -- having had -- a book -- a soma -- ten -- " -- having -- **** . Other composition is the same as that of the above-mentioned main phone SO fundamentally.
[0127] next, the cordless handset concerning the 3rd operation gestalt -- the composition of SC" is explained using drawing 9
[0128] drawing 9 -- being shown -- as -- the -- three -- operation -- a gestalt -- starting -- a cordless handset -- SC -- " -- the -- one -- operation -- a gestalt -- it can set -- a book -- a soma -- 30 -- replacing with -- it should deliver and receive -- information -- temporary -- memorizing -- while -- a password -- storing -- a password -- storing -- the section -- 70 -- A -- having had -- RAM -- 70 -- the after-mentioned -- encryption -- a password -- a signal -- Stw -- other composition -- fundamental -- the above -- a cordless handset -- it is the same as that of SC
[0129] next, main phone SO" which has the above composition and a cordless handset -- password transmission operation of the 3rd operation gestalt in the radio communications system constituted by SC" is explained using drawing 10 and drawing 11 In addition, the flow chart shown in the flow chart shown in drawing 10 and drawing 11 mainly shows a controller 14 or the processing in 34.
[0130] Operation in introduction and main phone SO" is explained using drawing 8 and drawing 10 .
[0131] In case it judges whether it is cordless handset SC" by which setting registration of the cordless handset connected is carried out beforehand in main phone SO", a synchronizing signal and the public key signal Sko corresponding to a public key are first transmitted to the cordless handset connected (Step S40). In this case, the public key signal Sko corresponding to the public key beforehand stored in RAM60 will be transmitted through the transceiver section 1 as a transmitting means. At this time, it can transmit with a frequency-hopping method using the above-mentioned table f (refer to drawing 3 (b)).
[0132] Transmission of the public key signal Sko judges whether next, it shifted to the reception standby state (Step S41), and there was any call from the cordless handset connected (Step S42). And when it is judged whether the predetermined time beforehand set as (Step S42; NO) and the degree when there is no call passed (Step S43) and it has not passed, a reception standby state is continued as it is (Step S43; NO) (Step S41), and when a predetermined time passes, it shifts to a sleep (Step S43; YES) state (Step S44). And it is judged whether the predetermined time set up further beforehand in the state of sleep passed (Step S45). When having not passed, a sleep (Step S45; NO) state is continued (Step S44). It is judged whether when it passes, the power supply of main phone SO" is (Step S45; YES) and a degree with ** (Step S46). When it is **, processing is ended as it is (Step S46; YES), and when it is not **, it returns to Step S40 that the public key signal Sko etc. should be transmitted again (Step S46; NO). By this step S43 or processing of S46, at the time of reception standby, a predetermined time interval will be set and a synchronizing signal and the public key signal Sko will be transmitted repeatedly.
[0133] When there is a call from the cordless handset connected in judgment of Step S42, on the other hand, (Step S42; YES), Acquire the above-mentioned ID information from the cordless handset concerned (Step S47), and the below-mentioned encryption password signal Stw further transmitted from the cordless handset concerned is acquired through the transceiver section 1 (Step S48). In a decoder 61, it restores using the private key signal Ssc corresponding to the above-mentioned private key in which the encryption password signal Stw concerned is beforehand stored by RAM60, and the

password signal Spw is acquired (Step S49).
[0134] next, the cordless handset with which the acquired password signal Spw is outputted to a controller 14, and it is registered beforehand -- the password (the password concerned) in which SC" is shown what has been transmitted by the radio transmission from the outside -- it is not -- main phone SO" -- it is set up by operating the very thing whether it is a corresponding thing judges -- having (Step S50) -- a cordless handset -- the communication connected for not being (Step S50; NO) and cordless handset SC" which should be connected, when it is not a thing corresponding to the password in which SC" is shown is cut, and it returns to Step (Step S51) S40
[0135] on the other hand -- a cordless handset -- the purport to which connection is permitted noting that (Step S50; YES) and the cordless handset connected are cordless handset SC", when it is a thing corresponding to the password in which SC" is shown -- the cordless handset concerned -- SC" -- receiving -- transmitting (Step S52) -- a degree -- a cordless handset -- concrete communication is started between SC" (Step S53) at this time, you may communicate with a frequency-hopping method using the hop table for the above-mentioned radio (beforehand -- main phone SO" and a cordless handset -- SC" shall have)
[0136] And it is judged whether the predetermined time beforehand set up during continuation of communication passed (Step S54). It is judged whether when having not passed, the communication itself was completed to (Step S54; NO) and the degree (Step S55). When having ended, it returns to Step S40 to perform (Step S55; YES) and the next communication, and when communication is not completed, it continues as it is (Step S55; NO) (Step S53).
[0137] the demand signal (the above-mentioned public key signal Sko is included.) of the purport which transmits a password to (Step S54; YES) and a degree again on the other hand when a predetermined time passes in the judgment of Step S54 -- a cordless handset -- it transmits to SC" and returns to Step (Step S56) S47 The check of a password will be repeated for every predetermined time during continuation of communication by operation of these steps S54 and S56.
[0138] next, the cordless handset corresponding to operation of above-mentioned main phone SO" -- password transmission operation in SC" is explained using drawing 9 and drawing 11
[0139] In SC" the cordless handset which should transmit a password corresponding to operation of above-mentioned main phone SO" -- Introduction, the synchronizing signal (drawing 10 step S40 reference) transmitted from main phone SO", and the public key signal Sko are received in the transceiver section 20 (Step S60). Next, the password which acquires the received public key signal Sko in this soma 30", and is stored in password storing section 70A in the code machine 71 using this (it is the same password as what is registered in main phone SO".) The corresponding password signal Si is enciphered and the encryption password signal Stw is generated (Step S61). the encryption in Step S61 -- setting -- the [the 1st or] -- like 2 operation forms, cipher systems, such as a RSA code in a public key cryptosystem, an ElGamal code, a elliptic curve cryptosystem, an ellipse RSA code, or an inverse number code, are used, and encryption is performed
[0140] Next, a call signal is transmitted to main phone SO" (Step S62.). drawing 10 step S42 reference -- continuing -- the cordless handset concerned -- the above-mentioned ID information on SC" is transmitted (Step S63.) Drawing 10 step S47 reference.
[0141] Then, the above-mentioned encryption password signal Stw is transmitted through the transceiver section 20 (Step S64.). Drawing 10 step S48 reference. At this time, you may transmit with a frequency-hopping method using the above-mentioned table f.
[0142] Next, it is if the above-mentioned connection enabling signal from main phone SO" is received (Step S65.). Drawing 10 step S52 reference and communication concrete between main phone SO" are started (Step S66.). Drawing 10 step S53 reference. At this time, you may communicate with a frequency-hopping method using the hop table for the above-mentioned radio.
[0143] Next, when it is judged whether there was any Request to Send (drawing 10 step S56 reference) of a password more nearly periodical than main phone SO" (Step S67) and it occurs (Step S67; YES), the above-mentioned steps S61 and S64 are processed, the encryption password signal Stw is transmitted to main phone SO", and it returns to Step S66 that communication should be continued.

[0144] On the other hand, in the judgment of Step S67, when there is no Request to Send of a password, it is judged whether communication was completed to (Step S67; NO) and the degree (Step S68) and it is not completed, communication is continued as it is (Step S68; NO) (Step S66), and when having ended, it shifts to a sleep (Step S68; YES) state (Step S69). and a cordless handset -- when it is judged whether the power supply of SC" became ** (Step S70) and it does not serve as **, a sleep state is continued as it is (Step S70; NO) (Step S69), and when it becomes **, processing (Step S70; YES) is ended

[0145] the cordless handset which learning of the password should not be carried out outside and should be certainly connected since according to operation of the radio communications system of the 3rd operation form explained above a password is enciphered, it transmits to main phone SO" and this is decoded -- SC" can be discriminated, and information can be delivered and received

[0146] Moreover, since it enciphers using a public key cryptosystem, a password and the secrecy nature of transfer of the information on subsequent can be raised further.

[0147] In addition, in the above-mentioned 3rd operation form, if the public key contained in the password Request-to-Send signal (drawing 10 step S56 reference) for every [from main phone SO"] fixed time is changed into the degree of a demand signal each time, the secrecy nature of a password will improve further.

[0148] Furthermore, after receiving ID information from cordless handset SC" in main phone SO" (drawing 10 step S47 reference) for example, a random number -- a cordless handset -- the cordless handset which transmitted to SC" and received this, while SC" enciphers what added the random number to the password using the public key from main phone SO" and making it transmit to main phone (drawing 11 step S64 reference) SO" main phone SO" which received this -- setting -- a private key -- restoring (drawing 10 step S49 reference) -- it can also constitute so that a random number may be deducted and a password may be acquired thus -- if it carries out -- a cordless handset -- the contents of the encryption password signal Stw which SC" transmits to main phone SO" will differ each time, and the secrecy nature of a password improves further

[0149] Furthermore, the information which should be delivered and received by the radio communications system of each operation form although only the portion about informational transfer was explained in each above-mentioned operation form may be the speech information which may be facsimile information by which facsimile transmission and reception should be carried out, and should be transmitted and received by the telephone again, for example. Furthermore, you may be the information which should be delivered and received between a computer and printers (or facsimile apparatus etc.). In this case, the main phone or cordless handset in each operation form will be carried in facsimile, telephone or a computer, and a printer, respectively. And when it consists of the codecs and compressors which perform the interconversion of voice and digital information when telephone is equipped with the main phone or the cordless handset, and dealing with the information on a computer etc. in a main phone or a cordless handset, it is constituted from the data converter which performs a buffer and error correction processing by the composition of the interface in each operation form.

[0150] Furthermore, transmission of the encryption table signal Sta in an above-mentioned operation form, the encryption initial value signal Sia, or the encryption password signal Stw may be performed as registration mode, only when newly registering a cordless handset, and you may be made to perform it each time at the time of a communication start.

[0151] Moreover, the creation information for generation of a hop table is transmitted timely during communication, and you may make it raise secrecy nature further.

[0152]

[Effect of the Invention] since information acquires canceling secrecy-ization using the secrecy-ized information which enciphered the secrecy-ized information for secrecy-izing the information itself which should be delivered and received, transmitted to the cordless handset from the main phone, and restored in the cordless handset according to invention according to claim 1 as having explained above -- the case of only secrecy-izing of the information itself -- comparing -- a main phone and a cordless handset -- between or a cordless handset -- the secrecy nature of the information in transfer between

comrades improves
[0153] Moreover, since the secrecy-ized information for transfer is enciphered and it transmits to the cordless handset concerned even when newly adding the cordless handset which does not have secrecy-ized information beforehand and starting informational transfer, secrecy-ized information is not revealed outside and the secrecy nature in informational transfer improves.
[0154] after according to invention according to claim 2 enciphering identification information, transmitting based on cryptographic key information, receiving this and restoring -- a setup -- since it distinguishes whether it is a cordless handset, although learning of the identification information is carried out outside -- things -- there is nothing -- certain -- a setup -- a cordless handset can be discriminated, and information can be delivered and received
[0155] therefore, a setup -- a cordless handset -- it can prevent that information is transmitted to the cordless handset of an except, and informational secrecy nature can be raised further
[0156] since information is acquired canceling secrecy-ization using the secrecy-ized information which enciphered the secrecy-ized information for secrecy-izing the information itself which should be delivered and received, transmitted to the cordless handset from the main phone, and was restored in the cordless handset according to invention according to claim 3 -- the case of only secrecy-izing of the information itself -- comparing -- a main phone and a cordless handset -- between or a cordless handset -- the secrecy nature of the information in transfer between comrades improves
[0157] Moreover, since the secrecy-ized information for transfer is enciphered and it transmits to the cordless handset concerned even when newly adding the cordless handset which does not have secrecy-ized information beforehand and starting informational transfer, secrecy-ized information is not revealed outside and the secrecy nature in informational transfer improves.
[0158] While according to invention according to claim 4 in addition to an effect of the invention according to claim 3 informational secrecy-ization changes in time the frequency used for transfer of the information concerned and is performed Since it is the table information referred to when secrecy-ized information changes frequency, information can be kept secret still more effectively to tapping etc. by secrecy-izing transfer of table information and performing it.
[0159] According to invention according to claim 5, in addition to an effect of the invention according claim 3 or 4, since decode key information is a private key in a public key cryptosystem while cryptographic key information is a public key in a public key cryptosystem, informational secrecy nature can be raised further.
[0160] While being the creation information for generating the table information referred to when secrecy-ized information changes frequency in addition to an effect of the invention according to claim 4 or 5 according to invention according to claim 6 Since it has further a generation means for a cordless handset generating table information using the creation information concerned The information which acquired table information and has been more quickly transmitted in a cordless handset as compared with the case where encipher the table information itself as secrecy-ized information, and it transmits to a cordless handset from a main phone can be decoded.
[0161] after according to invention according to claim 7 enciphering identification information, transmitting based on cryptographic key information, receiving this and restoring -- a setup -- since it distinguishes whether it is a cordless handset, learning of the identification information is carried out outside -- there is nothing -- certain -- a setup -- a cordless handset can be discriminated, and information can be delivered and received
[0162] therefore, a setup -- a cordless handset -- it can prevent that information is transmitted to the cordless handset of an except, and informational secrecy nature can be raised further
[0163] According to invention according to claim 8, in addition to an effect of the invention according claim 7, since decode key information is a private key in a public key cryptosystem while cryptographic key information is a public key in a public key cryptosystem, informational secrecy nature can be raised further.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the outline composition of the main phone of the 1st operation gestalt.
[Drawing 2] It is the block diagram showing the outline composition of the cordless handset of the 1st operation gestalt.
[Drawing 3] It is drawing showing the composition of a frame, and an example of a hop table, and (a) is drawing showing the composition of a frame, and (b) is drawing showing an example of a hop table.
[Drawing 4] It is the flow chart which shows operation of the main phone of the 1st operation gestalt.
[Drawing 5] It is the flow chart which shows operation of the cordless handset of the 1st operation gestalt.
[Drawing 6] It is the block diagram showing the outline composition of the main phone of the 2nd operation gestalt.
[Drawing 7] It is the block diagram showing the outline composition of the cordless handset of the 2nd operation gestalt.
[Drawing 8] It is the block diagram showing the outline composition of the main phone of the 3rd operation gestalt.
[Drawing 9] It is the block diagram showing the outline composition of the cordless handset of the 3rd operation gestalt.
[Drawing 10] It is the flow chart which shows operation of the main phone of the 3rd operation gestalt.
[Drawing 11] It is the flow chart which shows operation of the cordless handset of the 3rd operation gestalt.
[Description of Notations]
1 20 -- Transceiver section
2 21 -- Interface
3 22 -- Modulator and demodulator
4 23 -- Up converter
5 24 -- Power amplification
6 25 -- Transmission-and-reception circuit changing switch
7 26 -- Low noise amplifier
8 27 -- Down converter
9 28 -- PLL
10, 30, and 10' -- 30' and a 10 "30" -- book soma
11, 31, 40, 50, 60, 70 -- RAM
11A, 31A -- Hop table storing section
12 -- Code machine
13 33 -- Circuit changing switch
14 34 -- Controller
15 35 -- Power supply section

16 17 -- Frame
16A, 17A -- Frequency hop phase block
16B, 17D -- Transmitting phase block
16C, 17C -- Transmission-and-reception change phase block
16D, 17B -- Receiving phase block
32 -- Decoder
40A, 50A -- Initial value storing section
41 51 -- Hop table generation machine
60A, 70A -- Password storing section
SO, SO', SO" -- Main phone
SC, SC', SC" -- Cordless handset
Stt -- Table signal
Sif -- Information signal
Sta -- Encryption table signal
Sko -- Public key signal
Ssw1, Ssw2, Sm, Spl -- Control signal
Sc -- Local signal
St -- Sending signal
Sr -- Input signal
Smi -- Modulating signal
Sni -- Recovery signal
Ssc -- Private key signal
Si -- Initial value signal
Sia -- Encryption initial value signal
Spw -- Password signal
Stw -- Encryption password signal
ANT -- Antenna

[Translation done.]

CLAIMS

[Claim(s)]
[Claim 1] between the main phones and cordless handsets which are characterized by providing the following, or the cordless handset concerned -- the radio method for performing it on radio, decoding transfer of the information between comrades, while secrecy-izing the information concerned using secrecy-ized information the information secrecy-ized [aforementioned] from the aforementioned main phone -- the above -- the above which does not have the secrecy-ized information concerned for the aforementioned secrecy-ized information for receiving in a cordless handset, and canceling and decoding the secrecy-ization concerned from the aforementioned main phone -- the cryptographic key information for enciphering the secrecy-ized information concerned, when transmitting to a cordless handset -- the above -- the cryptographic key information transmitting process which transmits from a cordless handset to the aforementioned main phone The encryption process which enciphers the aforementioned secrecy-ized information in the aforementioned main phone based on the cryptographic key information which carried out [aforementioned] reception, and generates enciphered secrecy-ized information the enciphered secrecy-ized information by which generation was carried out [aforementioned] -- the above from the aforementioned main phone -- the secrecy-ized information transmitting process transmitted to a cordless handset the above -- the restoration process which decodes the enciphered secrecy-ized information by which transmission was carried out [aforementioned] in a cordless handset using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and restores the aforementioned secrecy-ized information
[Claim 2] a setup to which the cordless handset concerned between the main phones and cordless handsets which are characterized by providing the following was beforehand set in the main phone concerned, while performing transfer of the identification information for discriminating whether it is a cordless handset on radio, secrecy-izing the identification information concerned the aforementioned main phone and the aforementioned setup -- the cryptographic key information for being the radio method for delivering and receiving the information between cordless handsets on radio, and enciphering the aforementioned identification information -- the above from the aforementioned main phone -- the cryptographic key information transmitting process transmitted to a cordless handset, and the above -- a cordless handset The encryption process which enciphers the aforementioned identification information based on the cryptographic key information which carried out [aforementioned] reception, and generates encryption identification information the encryption identification information by which generation was carried out [aforementioned] -- the above -- the identification information transmitting process transmitted to the aforementioned main phone from a cordless handset The restoration process which decodes the encryption identification information by which transmission was carried out [aforementioned] in the aforementioned main phone using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and restores the aforementioned identification information the above transmitted in the aforementioned encryption identification information in the aforementioned main phone based on the identification information by which restoration was carried out [aforementioned] -- a cordless handset -

- the aforementioned setup -- the judgment process which judges whether it is a cordless handset, and the above which transmitted the aforementioned encryption identification information -- a cordless handset -- the aforementioned setup -- the time of it being distinguished that it is a cordless handset -- the setup concerned from the aforementioned main phone -- the transmitting process which transmits the aforementioned information to a cordless handset

[Claim 3] between the main phones and cordless handsets which are characterized by providing the following, or the cordless handset concerned -- the radio communications system which performs it on radio, decoding transfer of the information between comrades while secrecy-izing the information concerned using secrecy-ized information the above -- the information which is the cryptographic key information transmitting means included in a cordless handset, and was secrecy-ized [aforementioned] from the aforementioned main phone -- the above -- the above which does not have the secrecy-ized information concerned from the aforementioned main phone for the aforementioned secrecy-ized information for receiving in a cordless handset, and canceling and decoding the secrecy-ization concerned -- the cryptographic key information transmitting means transmit the cryptographic key information for enciphering the secrecy-ized information concerned to the aforementioned main phone when transmitting to a cordless handset An encryption means to encipher the aforementioned secrecy-ized information based on the cryptographic key information which carried out [aforementioned] reception, and to generate enciphered secrecy-ized information while being contained in the aforementioned main phone the enciphered secrecy-ized information by which generation was carried out [aforementioned] while being contained in the aforementioned main phone -- the above -- a secrecy-ized information transmitting means to transmit to a cordless handset the above -- a restoration means to decode the enciphered secrecy-ized information by which transmission was carried out [aforementioned] using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and to restore the aforementioned secrecy-ized information while being contained in a cordless handset

[Claim 4] It is the radio communications system characterized by the aforementioned secrecy-ized information being table information referred to when changing the aforementioned frequency while secrecy-ization of the aforementioned information is performed by changing in time the frequency used for transfer of the information concerned in a radio communications system according to claim 3.

[Claim 5] It is the radio communications system characterized by being a private key [in / the aforementioned public key cryptosystem / in the aforementioned decode key information] while the aforementioned cryptographic key information is a public key in a public key cryptosystem in a radio communications system according to claim 3 or 4.

[Claim 6] while the aforementioned secrecy-ized information is the creation information for generating the table information referred to when changing the aforementioned frequency in a radio communications system according to claim 4 or 5 -- the above -- the radio communications system characterized by equipping a cordless handset with the generation means for generating the aforementioned table information using the creation information concerned further

[Claim 7] a setup to which the cordless handset concerned between the main phones and cordless handsets which are characterized by providing the following was beforehand set in the main phone concerned -- while performing transfer of the identification information for discriminating whether it is a cordless handset on radio, secrecy-izing the identification information concerned -- the aforementioned main phone and the aforementioned setup -- the radio communications system for delivering and receiving the information between cordless handsets on radio the cryptographic key information for being the cryptographic key information transmitting means included in the aforementioned main phone, and enciphering the aforementioned identification information -- the above -- a cryptographic key information transmitting means to transmit to a cordless handset the above -- an encryption means to encipher the aforementioned identification information based on the cryptographic key information which carried out [aforementioned] reception, and to generate encryption identification information while being contained in a cordless handset the above -- an identification information transmitting means to transmit the encryption identification information by which generation was carried out

[aforementioned] to the aforementioned main phone while being contained in a cordless handset While being contained in a restoration means to decode the encryption identification information by which transmission was carried out [aforementioned] using the decode key information corresponding to the aforementioned cryptographic key information set up beforehand, and to restore the aforementioned identification information while being contained in the aforementioned main phone, and the aforementioned main phone the above which transmitted the aforementioned encryption identification information based on the identification information by which restoration was carried out [aforementioned] -- a cordless handset -- the aforementioned setup, while being contained in a judgment means to judge whether it is a cordless handset, and the aforementioned main phone the above which transmitted the aforementioned encryption identification information -- a cordless handset -- the aforementioned setup -- the time of it being distinguished that it is a cordless handset -- the setup concerned -- a transmitting means to transmit the aforementioned information to a cordless handset [Claim 8] It is the radio communications system characterized by being a private key [in / the aforementioned public key cryptosystem / in the aforementioned decode key information] while the aforementioned cryptographic key information is a public key in a public key cryptosystem in a radio communications system according to claim 7.

[Translation done.]

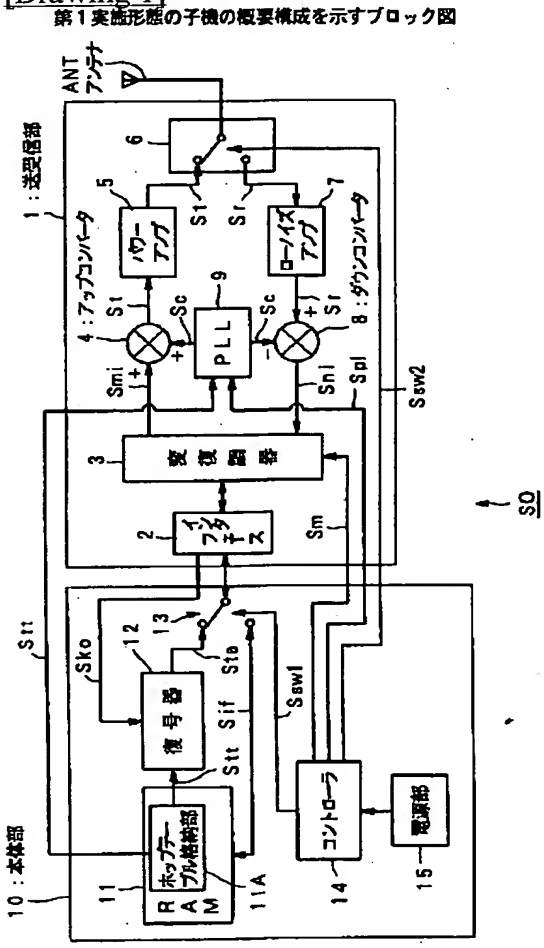
* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

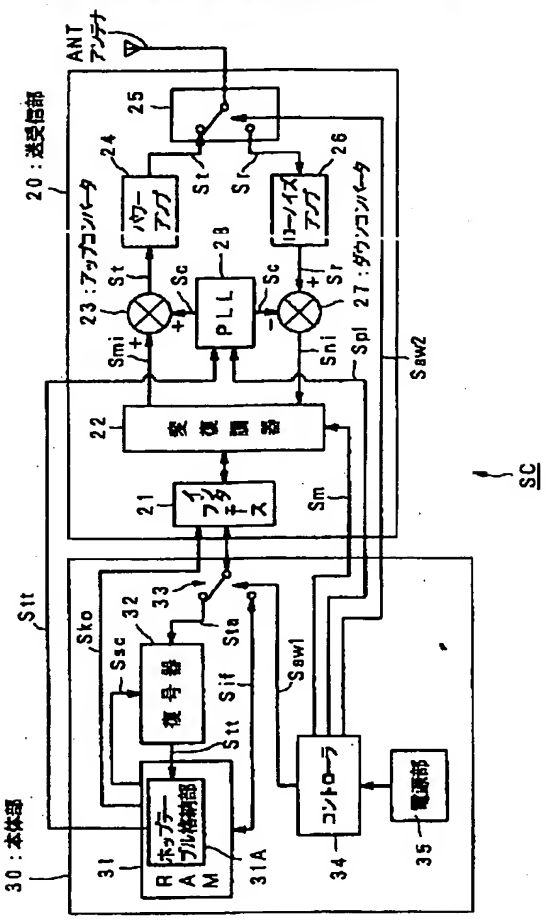
DRAWINGS

[Drawing 1]

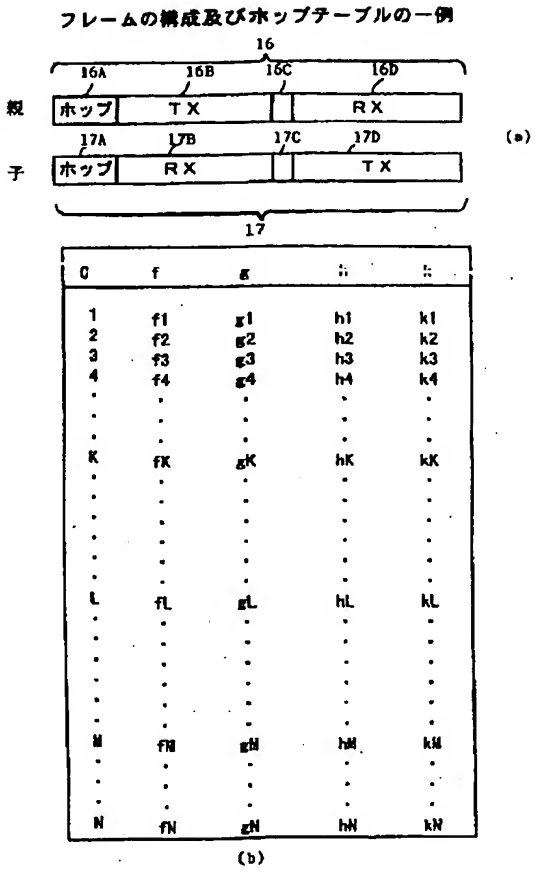


[Drawing 2]

第１実施形態の子機の概要構成を示すブロック図

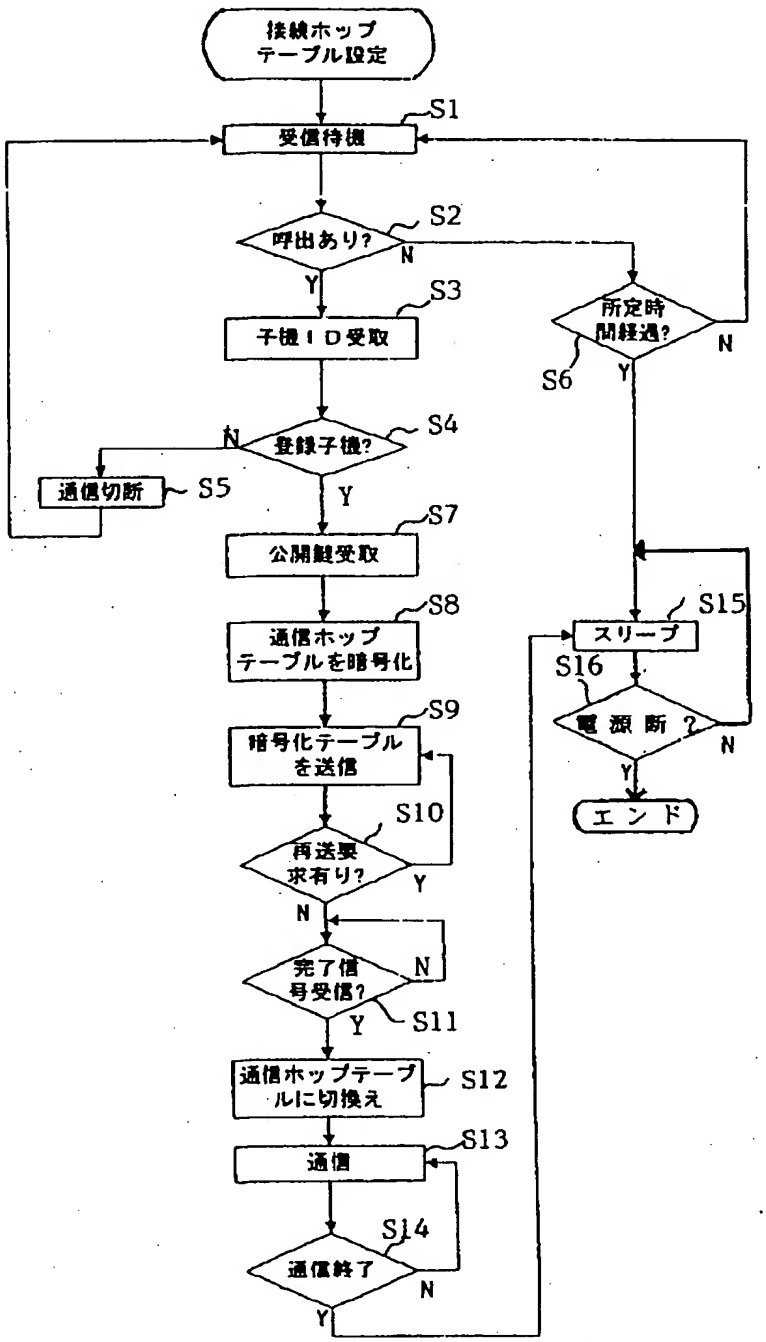


[Drawing 3]


フレームの構成及びホップテーブルの一例
16
16A
16B
16C
16D
親
ホップ
TX
RX
17A
17B
17C
17D
子
ホップ
RX
TX
(a)
17
0
f
g
h
k
1
f1
g1
h1
k1
2
f2
g2
h2
k2
3
f3
g3
h3
k3
4
f4
g4
h4
k4
K
fK
gK
hK
kK
L
fL
gL
hL
kL
M
fM
gM
hM
kM
N
fN
gN
hN
kN
(b)

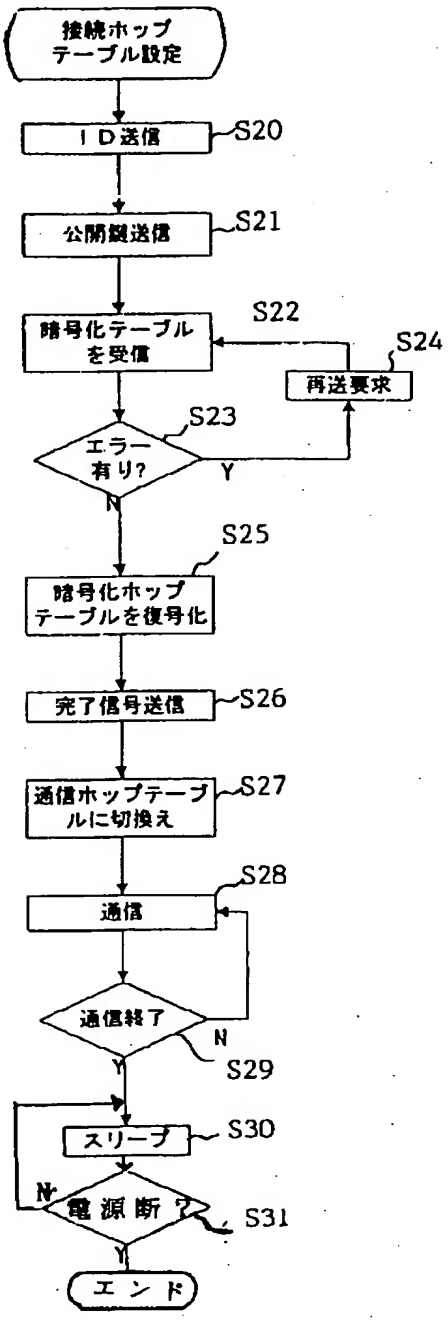
[Drawing 4]

第１実施形態の親機の動作を示すフローチャート



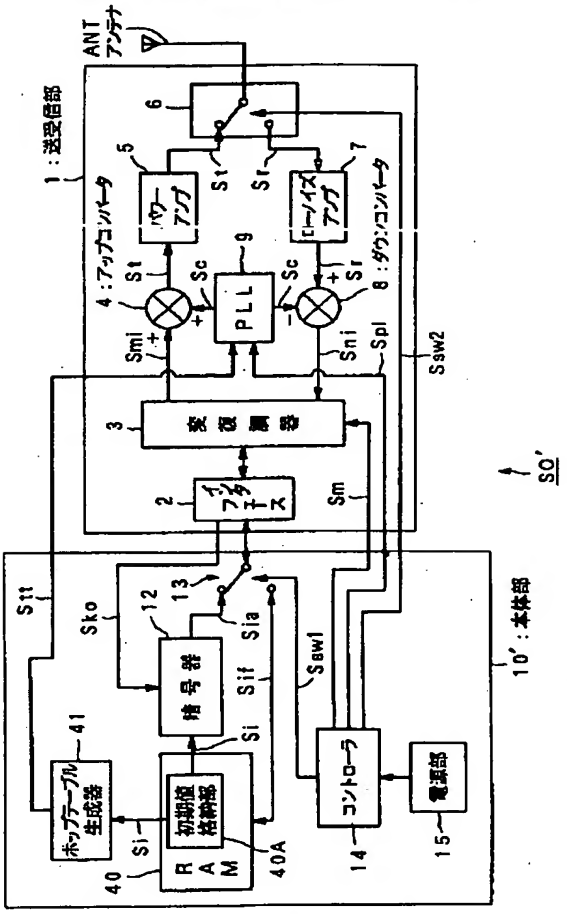
[Drawing 5]

第１実施形態の子機の動作を示すフローチャート

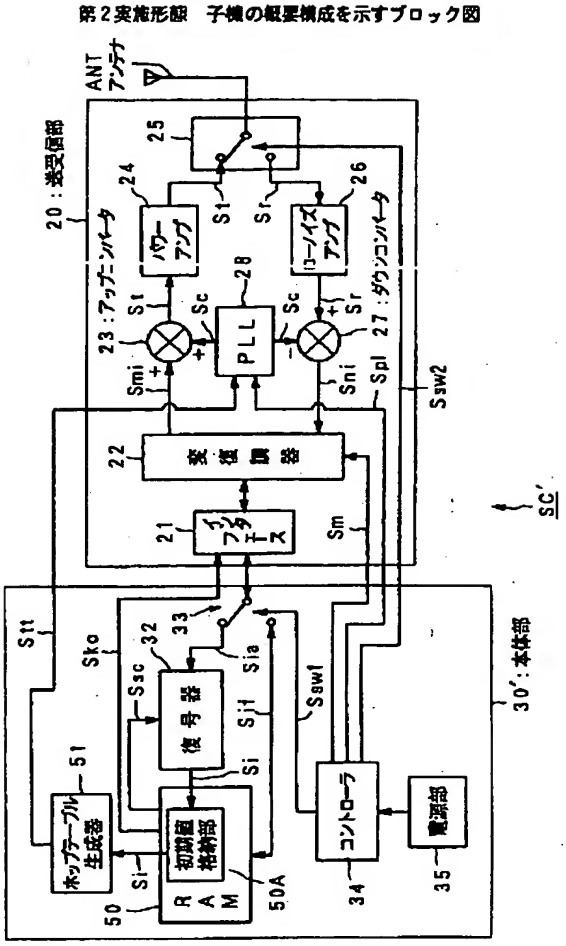


[Drawing 6]

第２実施形態の親機の概要構成を示すブロック図

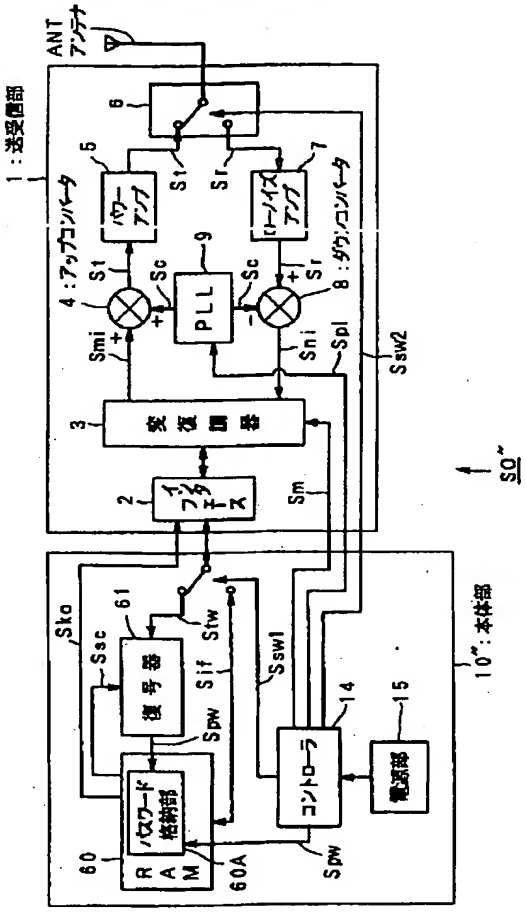


[Drawing 7]


第2実施形態　子機の概要構成を示すブロック図
ANT
アンテナ
20：送受信部
25
24
パワーアンプ
26
ローノイズアンプ
23：アップコンバータ
27：ダウンコンバータ
28
PLL
Smi
Sni
Spl
Ssw2
22
受信回路
21
インタフェース
Sm
SC'
Stt
Sko
32
33
Ssc
Sia
Sif
Si
Ssw1
復号器
51
ホップテーブル生成器
初期値格納部
RAM
50
50A
コントローラ
34
電源部
35
30'：本体部

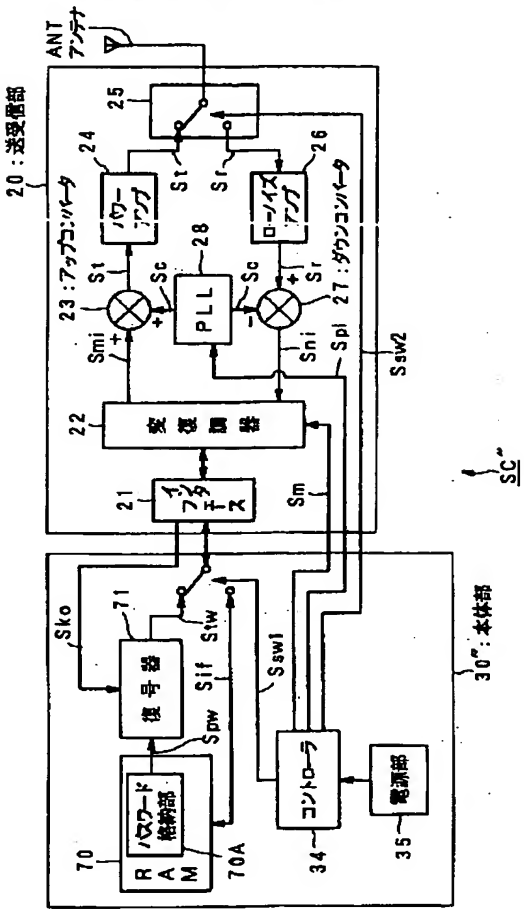
[Drawing 8]

第３実施形態の親機の概要構成を示すブロック図



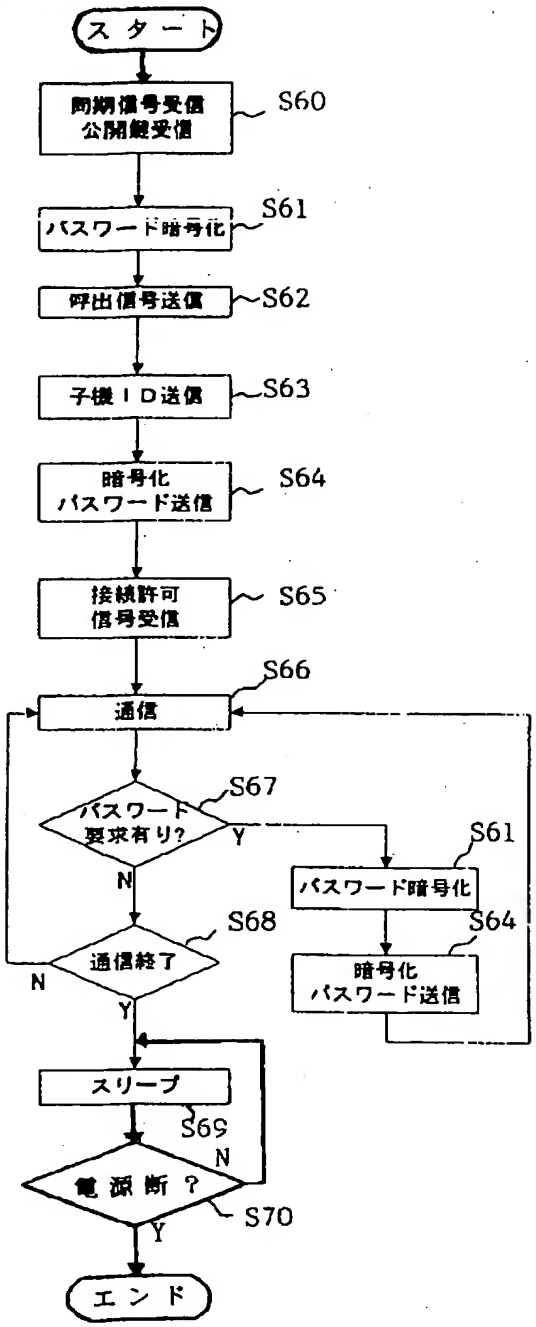
[Drawing 9]

第３実施形態の子機の概要構成を示すブロック図



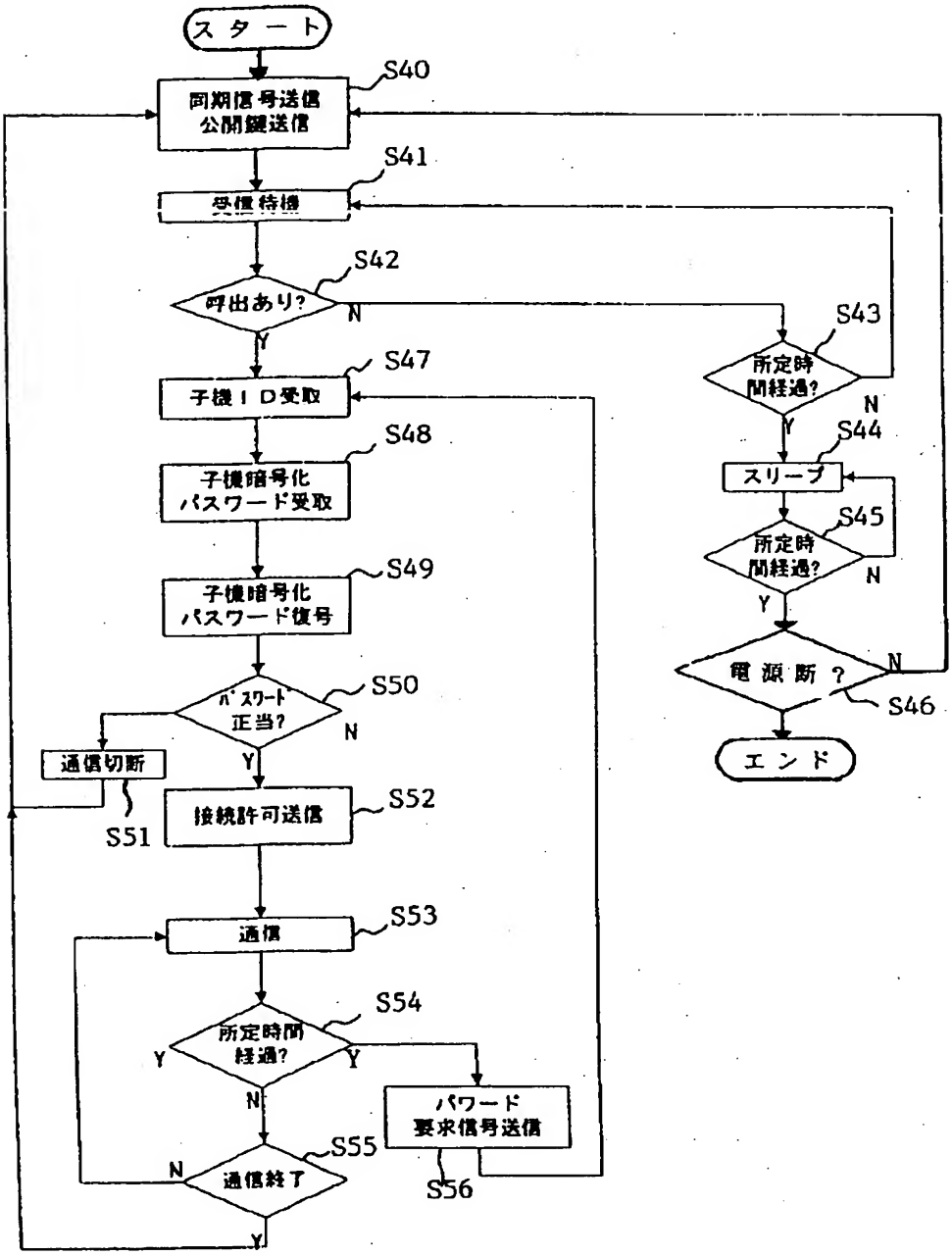
[Drawing 11]

第３実施形態の子機の動作を示すフローチャート



[Drawing 10]

第３実施形態の親機の動作を示すフローチャート



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－224340

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
Ｈ０４Ｑ　7/38		Ｈ０４Ｋ　1/08	
Ｈ０４Ｂ　1/713		Ｈ０４Ｂ　7/26	１０９Ｒ
Ｈ０４Ｋ　1/08		Ｈ０４Ｊ　13/00	Ｅ

審査請求　未請求　請求項の数８　ＯＬ　（全 20 頁）

(21)出願番号　特願平9－25456

(22)出願日　平成９年(1997)２月７日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

(72)発明者　滝　和也
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(74)代理人　弁理士　石川　泰男　（外２名）

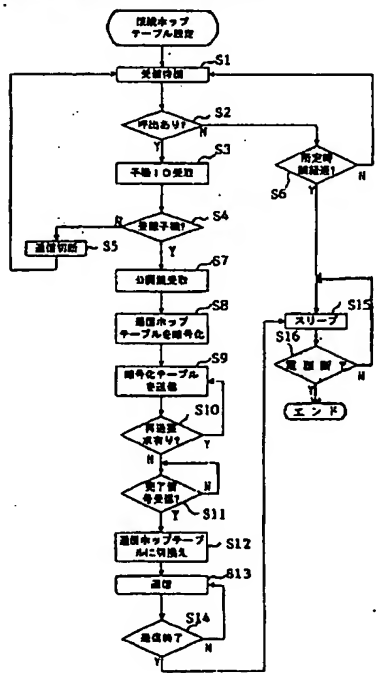
(54)【発明の名称】　無線通信方法及び無線通信システム

(57)【要約】

【課題】　親機と特定の子機との間における授受すべき情報の秘匿性を向上させることが可能な無線通信方法及び無線通信システムを提供する。

【解決手段】　第１の発明は、子機からの公開鍵（ステップＳ７）を用いて親機において周波数ホッピング方式におけるホップテーブルを公開鍵方式により暗号化し（ステップＳ８）、子機に送信し（ステップＳ９）、子機において秘密鍵を用いてこれを解読して復元し、親機と子機の双方においてホップテーブルを共有して周波数ホッピング方式により情報の授受を行う（ステップＳ１３）。第２の発明は、親機と子機夫々において、ホップテーブル生成器を備え、公開鍵暗号方式により暗号化した初期値のみを授受し、当該初期値を用いてホップテーブルを生成する。第３の発明は、子機を識別するパスワードを公開鍵暗号方式により暗号化して授受する。

第１実施形態の親機の動作を示すフローチャート



1

【特許請求の範囲】

【請求項１】　親機と子機との間又は当該子機同士間での情報の授受を、当該情報を秘匿化情報を用いて秘匿化すると共に復号しつつ無線で行うための無線通信方法であって、

前記親機からの前記秘匿化された情報を前記子機において受信して当該秘匿化を解除し復号するための前記秘匿化情報を、前記親機から当該秘匿化情報を有しない前記子機に対して送信するとき、当該秘匿化情報を暗号化するための暗号鍵情報を前記子機から前記親機に対して送信する暗号鍵情報送信工程と、

前記親機において、前記受信した暗号鍵情報に基づいて前記秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する暗号化工程と、

前記生成された暗号化済秘匿化情報を、前記親機から前記子機に送信する秘匿化情報送信工程と、

前記子機において、前記送信された暗号化済秘匿化情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記秘匿化情報を復元する復元工程と、

を備えることを特徴とする無線通信方法。

【請求項２】　親機と子機との間における、当該子機が当該親機において予め設定された設定子機であるか否かを識別するための識別情報の授受を、当該識別情報を秘匿化しつつ無線で行うと共に、前記親機と前記設定子機との間の情報の授受を無線で行うための無線通信方法であって、

前記識別情報を暗号化するための暗号鍵情報を前記親機から前記子機に対して送信する暗号鍵情報送信工程と、

前記子機において、前記受信した暗号鍵情報に基づいて前記識別情報を暗号化し、暗号化識別情報を生成する暗号化工程と、

前記生成された暗号化識別情報を前記子機から前記親機に送信する識別情報送信工程と、

前記親機において、前記送信された暗号化識別情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記識別情報を復元する復元工程と、

前記親機において、前記復元された識別情報に基づいて、前記暗号化識別情報を送信した前記子機が前記設定子機であるか否かを判断する判断工程と、

前記暗号化識別情報を送信した前記子機が前記設定子機であることが判別されたとき、前記親機から当該設定子機に対して前記情報を送信する送信工程と、

を備えることを特徴とする無線通信方法。

【請求項３】　親機と子機との間又は当該子機同士間での情報の授受を、当該情報を秘匿化情報を用いて秘匿化すると共に復号しつつ無線で行う無線通信システムであって、

前記子機に含まれる暗号鍵情報送信手段であって、前記親機からの前記秘匿化された情報を前記子機において受信して当該秘匿化を解除し復号するための前記秘匿化情報を、前記親機から当該秘匿化情報を有しない前記子機に対して送信するとき、当該秘匿化情報を暗号化するための暗号鍵情報を前記親機に対して送信する暗号鍵情報送信手段と、

前記親機に含まれると共に、前記受信した暗号鍵情報に基づいて前記秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する暗号化手段と、

前記親機に含まれると共に、前記生成された暗号化済秘匿化情報を前記子機に送信する秘匿化情報送信手段と、

前記子機に含まれると共に、前記送信された暗号化済秘匿化情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記秘匿化情報を復元する復元手段と、

を備えることを特徴とする無線通信システム。

【請求項４】　請求項３に記載の無線通信システムにおいて、

前記情報の秘匿化は、当該情報の授受に用いられる周波数を時間的に変化させて行われると共に、

前記秘匿化情報は、前記周波数を変化させる時に参照されるテーブル情報であることを特徴とする無線通信システム。

【請求項５】　請求項３又は４に記載の無線通信システムにおいて、

前記暗号鍵情報は、公開鍵暗号システムにおける公開鍵であると共に、

前記復号鍵情報は、前記公開鍵暗号システムにおける秘密鍵であることを特徴とする無線通信システム。

【請求項６】　請求項４又は５に記載の無線通信システムにおいて、

前記秘匿化情報は、前記周波数を変化させる時に参照されるテーブル情報を生成するための生成情報であると共に、

前記子機は、当該生成情報を用いて前記テーブル情報を生成するための生成手段を更に備えることを特徴とする無線通信システム。

【請求項７】　親機と子機との間における、当該子機が当該親機において予め設定された設定子機であるか否かを識別するための識別情報の授受を、当該識別情報を秘匿化しつつ無線で行うと共に、前記親機と前記設定子機との間の情報の授受を無線で行うための無線通信システムであって、

前記親機に含まれる暗号鍵情報送信手段であって、前記識別情報を暗号化するための暗号鍵情報を前記子機に対して送信する暗号鍵情報送信手段と、

前記子機に含まれると共に、前記受信した暗号鍵情報に基づいて前記識別情報を暗号化し、暗号化識別情報を生成する暗号化手段と、

前記子機に含まれると共に、前記生成された暗号化識別情報を前記親機に送信する識別情報送信手段と、

前記親機に含まれると共に、前記送信された暗号化識別情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記識別情報を復元する復元手段と、
前記親機に含まれると共に、前記復元された識別情報に基づいて前記暗号化識別情報を送信した前記子機が前記設定子機であるか否かを判断する判断手段と、
前記親機に含まれると共に、前記暗号化識別情報を送信した前記子機が前記設定子機であることが判別されたとき、当該設定子機に対して前記情報を送信する送信手段と、
を備えることを特徴とする無線通信システム。
【請求項８】　請求項７に記載の無線通信システムにおいて、
前記暗号鍵情報は、公開鍵暗号システムにおける公開鍵であると共に、
前記復号鍵情報は、前記公開鍵暗号システムにおける秘密鍵であることを特徴とする無線通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は親機と一又は複数の子機との間における無線通信において、秘匿性を高めて情報が外部に漏洩することを防止しつつ当該情報の授受を行う無線通信方法及び無線通信システムの技術分野に属する。
【０００２】
【従来の技術】近年、いわゆる無線ＬＡＮ（Local Area Network）が普及しつつあるが、この無線ＬＡＮに用いられる通信変調方式の一つとして最近一般化しつつあるのが、いわゆるスペクトラム拡散通信方式である。このスペクトラム拡散通信方式は、授受すべき信号のエネルギーを、その信号がもつ本来の周波数よりも広い周波数範囲に拡散して伝送する通信方式であり、電力密度を低く抑えることができる等の利点がある。
【０００３】そして、このスペクトラム拡散通信方式の中の一方式として普及しつつあるのでが、周波数ホッピング方式である。この方式は時間と共に周波数を変化させつつ情報を伝送する方式で、ホッピングの周期より十分長い時間で考えると電力密度を最も低く抑えられる利点があると共に、伝送する周波数が時々刻々と変化するので、妨害や盗聴に対しても耐性が高いという利点を有している。
【０００４】上記周波数ホッピング方式を用いた無線通信においては、情報を送信する送信無線局と情報を受信する受信無線局の双方においてホッピングする周波数を同期させるために、変化する周波数を示すいわゆるホップテーブルを双方で共通に保有し、このホップテーブルに従って送信無線局と受信無線局において送信周波数及び受信周波数を変化させつつ情報の授受を行う構成となっている。
【０００５】この時、送信無選局に対して受信無選局を増設する時、相互に周波数ホッピング方式を用いた情報の授受を開始する際には、予め上記ホップテーブルを送信無選局から受信無選局に送信して受信無選局において当該送信されたホップテーブルを用いて情報の授受を開始することが必要である。
【０００６】一方、例えば、予め設定された特定の受信無線局と送信無線局との間で情報の授受を行う場合には、受信無線局から特定のいわゆるパスワードを予め送信無線局に送信し、当該パスワードを送信無線局で取得してこれを復号し、上記特定の受信無線局であることを判別した上で当該受信無線局に対しての情報の送信を開始することが一般的である。
【０００７】
【発明が解決しようとする課題】しかしながら、情報の授受前における親機からの上記ホップテーブルの送信中に当該ホップテーブルが傍受されると、当該ホップテーブルを第三者が取得できることとなり、これにより、周波数ホッピング方式における情報の秘匿性が著しく低下することとなる場合があるという問題点があった。
【０００８】また、上記パスワードの受信無線局から送信無線局への送信において当該パスワードが傍受されると、当該パスワードを第三者が取得できることとなり、これにより、上記特定の受信無線局以外の他の無線局が恰も特定の受信無線局として情報を受信することができるようになり、この場合にも授受すべき情報の秘匿性が著しく低下することとなる。
【０００９】これらの問題点を回避すべく、上記ホップテーブル又はパスワード以外の、送信無線局と受信無線局との間で授受すべき情報そのものを暗号化することも考えられるが、この場合には、情報の暗号化及び復号化に大規模な演算が必要となると共にそのための回路構成も複雑化し、また、演算規模を縮小化するために簡易な暗号化とすると逆に秘匿性が低下してしまうという問題点が生じてくる。
【００１０】そこで、本発明は、上記の各問題点に鑑みてなされたもので、その課題は、電話回線等の外部回線に接続され専ら固定されて用いられる送信無線局（以下、親機という。）と特定の、例えば移動可能な受信無線局（以下、子機という。）との間における授受すべき情報の秘匿性を向上させることが可能な無線通信方法及び無線通信システムを提供することにある。
【００１１】
【課題を解決するための手段】上記の課題を解決するために、請求項１に記載の発明は、親機と子機との間又は当該子機同士間での情報の授受を、当該情報をホップテーブル等の秘匿化情報を用いて秘匿化すると共に復号しつつ無線で行うための無線通信方法であって、前記親機からの前記秘匿化された情報を前記子機において受信して当該秘匿化を解除し復号するための前記秘匿化情報

を、前記親機から当該秘匿化情報を有しない前記子機に対して送信するとき、当該秘匿化情報を暗号化するための暗号鍵情報を前記子機から前記親機に対して送信する暗号鍵情報送信工程と、前記親機において、前記受信した暗号鍵情報に基づいて前記秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する暗号化工程と、前記生成された暗号化済秘匿化情報を、前記親機から前記子機に送信する秘匿化情報送信工程と、前記子機において、前記送信された暗号化済秘匿化情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記秘匿化情報を復元する復元工程と、を備える。

【００１２】請求項１に記載の発明の作用によれば、暗号鍵情報送信工程において、秘匿化情報を親機から当該秘匿化情報を有しない子機に対して送信するとき、当該秘匿化情報を暗号化するための暗号鍵情報を子機から親機に対して送信する。

【００１３】次に、暗号化工程において、親機にて受信した暗号鍵情報に基づいて秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する。

【００１４】そして、秘匿化情報送信工程において、生成された暗号化済秘匿化情報を、親機から子機に送信する。

【００１５】次に、復元工程において、送信された暗号化済秘匿化情報を、子機にて暗号鍵情報に対応する復号鍵情報を用いて復号し、秘匿化情報を復元する。

【００１６】よって、授受すべき情報自体を秘匿化するための秘匿化情報を暗号化して親機から子機に送信し、子機において復元した秘匿化情報を用いて秘匿化を解除しつつ情報を取得するので、情報自体の秘匿化のみの場合に比して親機と子機間又は子機同士間の授受における情報の秘匿性が向上する。

【００１７】また、予め秘匿化情報を有しない子機を新たに加えて情報の授受を開始する場合でも、授受のための秘匿化情報を暗号化して当該子機に送信するので、秘匿化情報が外部に漏洩することがなく、情報の授受における秘匿性が向上する。

【００１８】上記の課題を解決するために、請求項２に記載の発明は、親機と子機との間における、当該子機が当該親機において予め設定された設定子機であるか否かを識別するためのパスワード等の識別情報の授受を、当該識別情報を秘匿化しつつ無線で行うと共に、前記親機と前記設定子機との間の情報の授受を無線で行うための無線通信方法であって、前記識別情報を暗号化するための暗号鍵情報を前記親機から前記子機に対して送信する暗号鍵情報送信工程と、前記子機において、前記受信した暗号鍵情報に基づいて前記識別情報を暗号化し、暗号化識別情報を生成する暗号化工程と、前記生成された暗号化識別情報を前記子機から前記親機に送信する識別情報送信工程と、前記親機において、前記送信された暗号化識別情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記識別情報を復元する復元工程と、前記親機において、前記復元された識別情報に基づいて、前記暗号化識別情報を送信した前記子機が前記設定子機であるか否かを判断する判断工程と、前記暗号化識別情報を送信した前記子機が前記設定子機であることが判別されたとき、前記親機から当該設定子機に対して前記情報を送信する送信工程と、を備える。

【００１９】請求項２に記載の発明の作用によれば、暗号鍵情報送信工程において、親機から暗号鍵情報を子機に対して送信する。

【００２０】そして、暗号化工程において、受信した暗号鍵情報に基づいて識別情報を子機にて暗号化し、暗号化識別情報を生成する。

【００２１】次に、識別情報送信工程において、生成された暗号化識別情報を子機から親機に送信する。

【００２２】その後、復元工程において、送信された暗号化識別情報を復号鍵情報を用いて親機にて復号し、識別情報を復元する。

【００２３】そして、判断工程において、復元された識別情報に基づいて暗号化識別情報を送信した子機が設定子機であるか否かを親機にて判断する。

【００２４】最後に、送信工程において、暗号化識別情報を送信した子機が設定子機であることが判別されたとき、親機から当該設定子機に対して情報を送信する。

【００２５】よって、識別情報が外部に知得されるがことなく、確実に設定子機を識別して情報の授受を行うことができる。

【００２６】上記の課題を解決するために、請求項３に記載の発明は、親機と子機との間又は当該子機同士間での情報の授受を、当該情報をホップテーブル等の秘匿化情報を用いて秘匿化すると共に復号しつつ無線で行う無線通信システムであって、前記子機に含まれる暗号鍵情報送信手段であって、前記親機からの前記秘匿化された情報を前記子機において受信して当該秘匿化を解除し復号するための前記秘匿化情報を、前記親機から当該秘匿化情報を有しない前記子機に対して送信するとき、当該秘匿化情報を暗号化するための暗号鍵情報を前記親機に対して送信する送受信部等の暗号鍵情報送信手段と、前記親機に含まれると共に、前記受信した暗号鍵情報に基づいて前記秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する暗号器等の暗号化手段と、前記親機に含まれると共に、前記生成された暗号化済秘匿化情報を前記子機に送信する送受信部等の秘匿化情報送信手段と、前記子機に含まれると共に、前記送信された暗号化済秘匿化情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記秘匿化情報を復元する復号器等の復元手段と、を備える。

【００２７】請求項３に記載の発明の作用によれば、子機に含まれる暗号鍵情報送信手段は、秘匿化情報を親機から当該秘匿化情報を有しない子機に対して送信すると

き、当該秘匿化情報を暗号化するための暗号鍵情報を親機に対して送信する。

【００２８】そして、親機に含まれる暗号化手段は、受信した暗号鍵情報に基づいて秘匿化情報を暗号化し、暗号化済秘匿化情報を生成する。

【００２９】その後、親機に含まれる秘匿化情報送信手段は、生成された暗号化済秘匿化情報を子機に送信する。

【００３０】最後に、子機に含まれる復元手段は、送信された暗号化済秘匿化情報を復号鍵情報を用いて復号し、秘匿化情報を復元する。

【００３１】よって、授受すべき情報自体を秘匿化するための秘匿化情報を暗号化して親機から子機に送信し、子機において復元した秘匿化情報を用いて秘匿化を解除しつつ情報を取得するので、情報自体の秘匿化のみの場合に比して親機と子機間又は子機同士間の授受における情報の秘匿性が向上する。

【００３２】また、予め秘匿化情報を有しない子機を新たに加えて情報の授受を開始する場合でも、授受のための秘匿化情報を暗号化して当該子機に送信するので、秘匿化情報が外部に漏洩することがなく、情報の授受における秘匿性が向上する。

【００３３】上記の課題を解決するために、請求項４に記載の発明は、請求項３に記載の無線通信システムにおいて、前記情報の秘匿化は、当該情報の授受に用いられる周波数を時間的に変化させて行われると共に、前記秘匿化情報は、前記周波数を変化させる時に参照されるテーブル情報であるように構成される。

【００３４】請求項４に記載の発明の作用によれば、請求項３に記載の発明の作用に加えて、情報の秘匿化が、当該情報の授受に用いられる周波数を時間的に変化させて行われると共に、秘匿化情報が周波数を変化させる時に参照されるテーブル情報であるので、テーブル情報の授受を秘匿化して行うことにより盗聴等に対して情報を更に効果的に秘匿することができる。

【００３５】上記の課題を解決するために、請求項５に記載の発明は、請求項３又は４に記載の無線通信システムにおいて、前記暗号鍵情報は、公開鍵暗号システムにおける公開鍵であると共に、前記復号鍵情報は、前記公開鍵暗号システムにおける秘密鍵であるように構成される。

【００３６】請求項５に記載の発明の作用によれば、請求項３又は４に記載の発明の作用に加えて、暗号鍵情報が公開鍵暗号システムにおける公開鍵であると共に、復号鍵情報が公開鍵暗号システムにおける秘密鍵であるので、更に情報の秘匿性を向上させることができる。

【００３７】上記の課題を解決するために、請求項６に記載の発明は、請求項４又は５に記載の無線通信システムにおいて、前記秘匿化情報は、前記周波数を変化させる時に参照されるテーブル情報を生成するための初期値等の生成情報であると共に、前記子機は、当該生成情報を用いて前記テーブル情報を生成するためのホップテーブル生成器等の生成手段を更に備える。

【００３８】請求項６に記載の発明の作用によれば、請求項４又は５に記載の発明の作用に加えて、秘匿化情報は周波数を変化させる時に参照されるテーブル情報を生成するための生成情報であると共に、子機が当該生成情報を用いてテーブル情報を生成するための生成手段を更に備える。

【００３９】よって、テーブル情報自体を秘匿化情報として暗号化して親機から子機に送信する場合に比してより迅速に子機においてテーブル情報を取得して送信されてきた情報を復号することができる。

【００４０】上記の課題を解決するために、請求項７に記載の発明は、親機と子機との間における、当該子機が当該親機において予め設定された設定子機であるか否かを識別するためのパスワード等の識別情報の授受を、当該識別情報を秘匿化しつつ無線で行うと共に、前記親機と前記設定子機との間の情報の授受を無線で行うための無線通信システムであって、前記親機に含まれる暗号鍵情報送信手段であって、前記識別情報を暗号化するための暗号鍵情報を前記子機に対して送信する送受信部等の暗号鍵情報送信手段と、前記子機に含まれると共に、前記受信した暗号鍵情報に基づいて前記識別情報を暗号化し、暗号化識別情報を生成する暗号器等の暗号化手段と、前記子機に含まれると共に、前記生成された暗号化識別情報を前記親機に送信する送受信部等の識別情報送信手段と、前記親機に含まれると共に、前記送信された暗号化識別情報を前記暗号鍵情報に対応する予め設定された復号鍵情報を用いて復号し、前記識別情報を復元する復号器等の復元手段と、前記親機に含まれると共に、前記復元された識別情報に基づいて前記暗号化識別情報を送信した前記子機が前記設定子機であるか否かを判断するコントローラ等の判断手段と、前記親機に含まれると共に、前記暗号化識別情報を送信した前記子機が前記設定子機であることが判別されたとき、当該設定子機に対して前記情報を送信する送受信部等の送信手段と、を備える。

【００４１】請求項７に記載の発明の作用によれば、親機に含まれる暗号鍵情報送信手段は、暗号鍵情報を子機に対して送信する。

【００４２】そして、子機に含まれる暗号化手段は、受信した暗号鍵情報に基づいて識別情報を暗号化し、暗号化識別情報を生成する。

【００４３】その後、子機に含まれる識別情報送信手段は、生成された暗号化識別情報を親機に送信する。

【００４４】次に、親機に含まれる復元手段は、送信された暗号化識別情報を復号鍵情報を用いて復号し、識別情報を復元する。

【００４５】そして、親機に含まれる判断手段は、復元

された識別情報に基づいて暗号化識別情報を送信した子機が設定子機であるか否かを判断する。

【００４６】最後に、親機に含まれる送信手段は、暗号化識別情報を送信した子機が設定子機であることが判別されたとき、当該設定子機に対して情報を送信する。

【００４７】よって、識別情報が外部に知得されることがなく、確実に設定子機を識別して情報の授受を行うことができる。

【００４８】上記の課題を解決するために、請求項８に記載の発明は、請求項７に記載の無線通信システムにおいて、前記暗号鍵情報は、公開鍵暗号システムにおける公開鍵であると共に、前記復号鍵情報は、前記公開鍵暗号システムにおける秘密鍵であるように構成される。

【００４９】請求項８に記載の発明の作用によれば、請求項７に記載の発明の作用に加えて、暗号鍵情報が公開鍵暗号システムにおける公開鍵であると共に、復号鍵情報が公開鍵暗号システムにおける秘密鍵であるので、更に情報の秘匿性を向上させることができる。

【００５０】

【発明の実施の形態】次に、本発明に好適な実施の形態について、図面を用いて説明する。

【００５１】（Ｉ）第１実施形態

始めに、本発明に係る第１の実施形態について、図１乃至図５を用いて説明する。ここで、以下に説明する第１実施形態は、予め親機と一又は複数個の子機により形成されると共に、周波数ホッピング方式を用いた無線通信システムに対して、新たに子機を加えて当該周波数ホッピング方式により情報の授受を開始する場合に本発明を適用した実施の形態である。

【００５２】先ず、本実施形態の無線通信システムを構成する親機の全体構成及び概要動作について、図１を用いて説明する。

【００５３】図１に示すように、親機ＳＯは、送信すべき情報等を生成すると共に受信した情報を処理する本体部１０と、送信すべき情報をアンテナＡＮＴを介して子機に送信すると共に、子機から送信されてきた情報を当該アンテナＡＮＴを介して受信し、本体部１０に出力する秘匿化情報送信手段としての送受信部１とにより構成されている。

【００５４】そして、送受信部１は、インターフェース２と、変復調部３と、アップコンバータ４と、パワーアンプ５と、送受切替スイッチ６と、ローノイズアンプ７と、ダウンコンバータ８と、ＰＬＬ（Phase Locked Loop）９と上記アンテナＡＮＴにより構成されている。

【００５５】また、本体部１０は、子機との間で授受すべき情報等を一時的に記憶するＲＡＭ（Random Access Memory）１１と、当該ＲＡＭ１１内に備えられ、ホップテーブルに含まれる情報を記憶するホップテーブル格納部１１Ａと、後述の処理においてホップテーブルを暗号化する暗号化手段としての暗号器１２と、暗号器１２の出力と上記授受すべき情報とを切り替えて送受信部１に出力する切替スイッチ１３と、親機ＳＯ全体を制御するコントローラ１４と、親機ＳＯの各構成部材に対してコントローラ１４を介して電源電圧を供給する電源部１５とにより構成されている。

【００５６】次に、本実施形態の無線通信システムを構成する子機の全体構成及び概要動作について、図２を用いて説明する。

【００５７】図２に示すように、子機ＳＣは、送信すべき情報等を生成すると共に受信した情報を処理する本体部３０と、送信すべき情報をアンテナＡＮＴを介して親機ＳＯに送信すると共に、親機ＳＯから送信されてきた情報を当該アンテナＡＮＴを介して受信し、本体部３０に出力する暗号鍵情報送信手段としての送受信部２０とにより構成されている。

【００５８】そして、送受信部２０は、インターフェース２１と、変復調部２２と、アップコンバータ２３と、パワーアンプ２４と、送受切替スイッチ２５と、ローノイズアンプ２６と、ダウンコンバータ２７と、ＰＬＬ（Phase Locked Loop）２８と上記アンテナＡＮＴにより構成されている。

【００５９】また、本体部３０は、親機との間で授受すべき情報等を一時的に記憶するＲＡＭ３１と、当該ＲＡＭ３１内に備えられ、ホップテーブルに含まれる情報を記憶するホップテーブル格納部３１Ａと、後述の処理において送信されてきたホップテーブルを復元する復元手段としての復号器３２と、復号器３２の出力と上記授受すべき情報とを切り替えて送受信部２０に出力する切替スイッチ３３と、子機ＳＣ全体を制御するコントローラ３４と、コントローラ３４を介して子機ＳＣの各構成部材に対して電源電圧を供給する電源部３５とにより構成されている。

【００６０】次に、親機ＳＯ及び子機ＳＣの細部動作について、図１乃至図５を用いて説明する。

【００６１】始めに、本実施形態の無線通信システムにおける一般の情報の授受（ホップテーブルが親機ＳＯ及び子機ＳＣにおいて取得されており、これに基づいて周波数ホッピング方式により実行される情報の授受）の動作について、図１乃至図３を用いて説明する。

【００６２】先ず、親機ＳＯから情報を送信し、子機ＳＣにおいてこれを受信する場合の処理について説明する。

【００６３】親機ＳＯから子機ＳＣに対して情報を送信する場合、図１に示すように、情報信号Ｓifを子機ＳＣに対して送信する際には、ＲＡＭ１１内のホップテーブル格納部１１Ａに格納されている上記ホップテーブルの情報がテーブル信号ＳttとしてＰＬＬ９に出力され、当該ＰＬＬ９においては、コントローラ１４からの制御信号Ｓplに基づきテーブル信号Ｓttを参照して当該ホップテーブルに設定されている周波数の局部信号Ｓcを生成

すると共に周波数ロックして上記アップコンバータ４に出力する。一方、当該送信すべき情報は一旦ＲＡＭ１１に蓄えられた後に情報信号Ｓifとして切替スイッチ１３に出力される。この時、当該切替スイッチ１３は、コントローラ１４からの制御信号Ssw_1に基づいて情報信号Ｓif側に切り替えられている。

【００６４】そして、当該情報信号Ｓifが切替スイッチ１３を介して送受信部１に出力されると、インターフェース２によって情報信号Ｓifの属性に対応して送受信部１への取り込み動作（インターフェース動作）が行われ、変復調器３において所定の変調が施されて変調信号Ｓmiとして出力され、アップコンバータ４に出力される。

【００６５】これらにより、ミキサ等により構成されているアップコンバータ４において、上記変調信号Ｓmiの周波数と局部信号Ｓcの周波数とが加算され、送信信号Ｓtとしてパワーアンプ５に出力され所定の増幅率で増幅される。その後、当該送信信号Ｓtが送受切替スイッチ６（コントローラ１４からの制御信号Ssw_2に基づいて送信信号Ｓt側に切り替えられている。）を介してアンテナＡＮＴから子機ＳＣに対して送信される。このアップコンバータ４の動作により、送信信号Ｓtを送信する時の周波数が、ホップテーブルとして設定されている周波数を含むように時間に対応して変化することとなる。

【００６６】次に、子機における受信動作について図２を用いて説明する。

【００６７】親機ＳＯから周波数を変化させつつ送信されてきた送信信号Ｓtを含む情報は、子機ＳＣにおけるアンテナＡＮＴにおいて受信され、送受切替スイッチ２５を介して受信信号ＳrとしてローノイズアンプＳ２６において所定の増幅率で増幅される。このとき、送受切替スイッチ２５は、コントローラ３４からの制御信号Ssw_2に基づいてローノイズアンプ２６側に切り替えられている。そして、ローノイズアンプにより増幅された受信信号Ｓrがダウンコンバータ２７に出力される。

【００６８】一方、親機ＳＯからの情報を子機ＳＣにおいて受信する際には、ＲＡＭ３１内のホップテーブル格納部３１Ａに格納されている上記ホップテーブル（親機ＳＯのホップテーブルと同じ内容を有している。）の情報がテーブル信号ＳttとしてＰＬＬ２８に出力され、当該ＰＬＬ２８においては、コントローラ３４からの制御信号Ｓplに基づきテーブル信号Ｓttを参照して当該ホップテーブルに設定されている周波数の局部信号Ｓcを上記ダウンコンバータ２７に出力する。

【００６９】これらにより、ミキサ等により構成されているダウンコンバータ２７において、上記受信信号Ｓrの周波数から局部信号Ｓcの周波数が減算され、親機ＳＯにおける変調信号Ｓmiと同様の信号である復調信号Ｓniとなって変復調器２２に出力され、当該変復調器２２において復調動作が実行されてインターフェース２１を介して本体部３０に出力される。

【００７０】その後、復調された信号は、本体部３０において切替スイッチ３３を介して情報信号Ｓifとして出力され、ＲＡＭ３１に一時的に記憶される。このとき、切替スイッチ３３は、コントローラ３４からの制御信号Ssw_1に基づいて情報信号Ｓif側に切り替えられている。

【００７１】その後は、図示しない処理部により、記憶している情報に対して所定の処理等が実行される。

【００７２】ここで、本実施形態における親機ＳＯと子機ＳＣとの間で送受信される情報の構造について図３を用いて説明する。

【００７３】本実施形態の無線通信システムにおいては、いわゆるＴＤＤ（時分割デュープレクス）方式を用いて双方向通信を行う。すなわち、例えば親機ＳＯから子機ＳＣに情報を送信する場合には、親機ＳＯは、図３（ａ）に示すように、周波数ホップフェーズブロック１６Ａ、送信フェーズブロック１６Ｂ、送受切替フェーズブロック１６Ｃ及び受信フェーズブロック１６Ｄからなるフレーム１６を単位として情報を構成して動作する。一方、子機ＳＣは、図３（ａ）に示すように、周波数ホップフェーズブロック１７Ａ、受信フェーズブロック１７Ｂ、送受切替フェーズブロック１７Ｃ及び送信フェーズブロック１７Ｄからなるフレーム１７を単位として情報を構成して動作する。この時、これらの各フェーズブロックは、夫々のフレーム内での開始から終了までのタイミングが予め設定されて管理されている。また、周波数のホッピング（切替）は各フレーム毎に行われ、一のフレームを構成する情報を送受信している時に周波数が変化することはない。

【００７４】これらのフェーズブロックの内、周波数ホップフェーズブロック１６Ａ及び１７Ａは、フレームの切り替えに伴って遷移状態となる送受信周波数を安定させる期間で、親機ＳＯ又は子機ＳＣ間で情報の送受信は行わない。

【００７５】また、親機ＳＯの送信フェーズブロック１６Ｂ（すなわち子機ＳＣの受信フェーズブロック１７Ｂ）では、親機ＳＯから子機ＳＣへ情報が送信される期間で、当該情報には、上記送信信号Ｓtの他に、制御信号として、親機ＳＯと子機ＳＣとのフレーム毎の同期を取るための同期信号、子機ＳＣを呼出すための呼出信号、子機ＳＣからの当該呼出を受け付けた旨を示す接続許可信号及び親機ＳＯが通信中である旨を示すビジー信号等が含まれている。

【００７６】更に、送受切替フェーズブロック１６Ｃ又は１７Ｃは、親機ＳＯ及び子機ＳＣの夫々において、送信と受信が入れ替わる遷移期間で、親機ＳＯ又は子機ＳＣ間で情報の送受信は行わない。

【００７７】最後に、親機ＳＯの受信フェーズブロック

１６Ｄ（すなわち子機ＳＣの送信フェーズブロック１７Ｄ）は、後述の動作により子機ＳＣから親機ＳＯへ情報が送信される期間で、当該情報には、後述の子機ＳＣにおける送信信号Ｓｔの他に、制御信号として、子機ＳＣ側で親機ＳＯとの同期が取れたことを返答する同期確認信号、親機ＳＯを呼出す呼出信号、親機ＳＯから呼出を受けた旨を示す接続了承信号及び子機ＳＣが通信中である旨を示すビジー信号等が含まれている。

【００７８】上述の各フェーズブロックにより構成されるフレームを単位として一つのフレームにおいて送受信が行われ、当該送受信が複数フレームに渡って繰返し実行されることにより親機ＳＯと子機ＳＣ間で双方向の通信が実行されることとなる。また、上記各フレームは、親機ＳＯ及び子機ＳＣにおける夫々のコントローラからの制御信号Ｓｍに基づいて構成されるものである。

【００７９】次に、子機ＳＣから情報を送信し、親機ＳＯにおいてこれを受信する場合の処理について説明する。

【００８０】子機ＳＣから親機ＳＯに対して情報を送信する場合の動作は、基本的には、上述の親機ＳＯから子機ＳＣに対して情報を送信する場合の動作における親機ＳＯと子機ＳＣを入れ替えた場合の処理と等価である。

【００８１】すなわち、子機ＳＣのＲＡＭ１１に記憶されている情報が、情報信号Ｓｉｆとして切替スイッチ３３、インターフェース２１及び変復調器２２を介して変調信号Ｓｍｉとしてアップコンバータ２３に出力される。そして、当該アップコンバータ２３においてＰＬＬ２８からのホップテーブル内の周波数情報に対応した局部信号Ｓｃの周波数が加算されてパワーアンプ２４において増幅され、送受切替スイッチ２５を介してアンテナＡＮＴから送信される。この時には、送受信のための周波数が上記フレーム毎に変化していることとなる。

【００８２】そして、親機ＳＯのアンテナＡＮＴにおいて受信された信号は、送受切替スイッチ６を介して受信信号Ｓｒとしてローノイズアンプ７において増幅され、ダウンコンバータ８において当該受信信号Ｓｒの周波数から局部信号Ｓｃの周波数が減算されて復調信号Ｓｎｉとなり、これが変復調器３において復調された後インターフェース２を介して本体部１０に送られ、切替スイッチ１３を介してＲＡＭ１１内に一時的に蓄えられる。

【００８３】以上説明した各部の動作により、周波数ホッピング方式を用いて親機ＳＯと子機ＳＣとの間で情報の双方向通信が実行されることとなる。

【００８４】次に、当該周波数ホッピング方式に用いられるホップテーブルについて、図３（ｂ）を用いて例示しつつ説明する。なお、図３（ｂ）は、ホップテーブルとして４種類のテーブル（Ｎ種類の周波数を夫々含むテーブルｆ乃至ｋ）が親機ＳＯにおけるホップテーブル格納部１１Ａに記憶されている状態を示している。

【００８５】この時、例えば、テーブルｆに記載されているＮ種類の周波数は、呼出制御又は後述のホップテーブル自体の親機ＳＯから子機ＳＣに伝送する際の周波数変更に用いられ、また、テーブルｇ乃至ｋに夫々記載されているＮ種類の周波数は、秘匿すべき情報を親機ＳＯから子機ＳＣに実際に伝送する際（情報通信時）の周波数変更に用いられる。この時、一のテーブルに含まれる周波数が一の子機ＳＣとの間での通信に用いられる。つまり、図３（ｂ）に示す場合には、一の親機ＳＯに対して３台の子機ＳＣを無線接続し、一の子機ＳＣに対してテーブルｇ乃至ｋのうち一のテーブルを割り当てて情報を送受信することが可能となる。

【００８６】次に、本発明に係る、親機ＳＯに新規に子機ＳＣを無線接続する際の上記ホップテーブルを親機ＳＯから子機ＳＣに伝送するための処理について、図１及び図２並びに図４及び図５に示すフローチャートを用いて説明する。なお、図４に示すフローチャートは親機ＳＯにおける処理を示すものであり、図５に示すフローチャートは子機ＳＣにおける処理を示すものであり、主としてコントローラ１４又は３４における処理を示すものである。

【００８７】始めに、親機ＳＯにおける動作について、図１及び図４を用いて説明する。

【００８８】新規な子機ＳＣに対して親機ＳＯから情報通信用のホップテーブル（例えば、図３（ｂ）におけるテーブルｇ乃至ｋのうちのいずれか一つのホップテーブル）を伝送する際には、始めに、受信待機（ステップＳ１）している親機ＳＯにおいて、当該新規に接続すべき子機ＳＣからの呼出があったか否かが判定され（ステップＳ２）、呼出があった場合には（ステップＳ２；ＹＥＳ）当該子機ＳＣからＩＤ情報（一の子機ＳＣを特定するための情報であり、毎フレーム毎にその先頭に含まれる情報である。このＩＤ情報は暗号化されずに送受信されるのが通常である。）を受け取る（ステップＳ３）。そして、受け取ったＩＤ情報により当該子機ＳＣが予め登録されている子機ＳＣ（ＩＤ情報は、親機ＳＯに接続可能な（将来において接続される可能性のある）子機ＳＣのＩＤ情報として予め登録されている。）のＩＤ情報であるか否かを判定する（ステップＳ４）。

【００８９】一方、ステップＳ２の判定において、子機ＳＣから呼出がないときは（ステップＳ２；ＮＯ）予め設定した所定の時間が経過したか否かが判定され（ステップＳ６）、経過していない時は（ステップＳ６；ＮＯ）受信待機状態（ステップＳ１）を継続し、経過している時は（ステップＳ６；ＹＥＳ）親機ＳＯをスリープ状態とする（ステップＳ１５）。

【００９０】また、ステップＳ４の判定において、登録してある子機ＳＣでない時は（ステップＳ４；ＮＯ）、予め接続を予定していた子機ＳＣでないとして当該子機ＳＣとの通信を断とし（ステップＳ５）そのまま受信待機すべくステップＳ１に戻る。

15

【００９１】更に、ステップＳ４の判定において、登録してある子機ＳＣである時は（ステップＳ４；ＹＥＳ）次に当該子機ＳＣから送信されてくる公開鍵信号Ｓkoを送受信部１において通常の情報と同様にして受信し（ステップＳ７）、当該受信した公開鍵信号Ｓkoに含まれている公開鍵情報を用いて、ホップテーブル格納部１１Ａに記憶されている情報通信用のホップテーブルのうちのいずれか一のホップテーブル（接続しようとしている子機ＳＣとの無線通信に用いられるべきホップテーブル）に対応するテーブル信号Ｓttを暗号器１２において暗号化し、暗号化テーブル信号Ｓtaを出力する（ステップＳ８）。その後、当該暗号化テーブル信号Ｓtaを送受信部１を介して子機ＳＣに送信する（ステップＳ９）。この時、切替スイッチ１３は、暗号器１２側に切り替わっている。また、暗号化テーブル信号Ｓtaを子機ＳＣに送信する際の周波数ホッピングには、図３（ｂ）に示すテーブルｆ（このテーブルのみは全ての子機ＳＣが予め備えている。）を用いて周波数が変更されつつ送信される。更に、ステップＳ８における暗号化においては、例えば、公開鍵暗号方式における、ＲＳＡ（Rivest-Shamir-Adleman）暗号、ElGamal暗号、楕円曲線暗号、楕円ＲＳＡ暗号又は逆数暗号等の暗号方式が用いられて暗号化が行われる。

【００９２】ここで、上記公開鍵とは、いわゆる公開鍵暗号方式において用いられるものであり、本実施形態においては、無線通信用のホップテーブルを取得すべき子機ＳＣが親機ＳＯに対して公開鍵に対応する公開鍵信号Ｓkoを送信し、これを受信した親機ＳＯにおいて当該公開鍵を用いて無線通信用のホップテーブルを暗号化し、当該暗号化したホップテーブルを子機ＳＣに送信する。そして、これを受信した子機ＳＣにおいては、上記公開鍵に対応している秘密鍵（公開鍵そのものとは異なるものである。）を用いて暗号を解読してホップテーブルを取得することとなる。

【００９３】暗号化テーブル信号Ｓtaを送信すると、次に、子機ＳＣから後述の暗号化テーブル信号Ｓtaの再送要求がないか否かを確認して（ステップＳ１０）、再送要求があった場合には（ステップＳ１０；ＹＥＳ）再送し（ステップＳ９）、再送要求がない時は（ステップＳ１０；ＮＯ）、次に子機ＳＣからの後述の受信完了信号を受信したか否かを確認し（ステップＳ１１）、受信していない時は（ステップＳ１１；ＮＯ）受信するまで待機する。

【００９４】一方、受信完了信号を受信した時は（ステップＳ１１；ＹＥＳ）、次にホップテーブルをそれまで使用していたテーブルｆから無線通信用のホップテーブル（暗号化して送信した（ステップＳ９）ホップテーブル）に切り替え（ステップＳ１２）、当該無線通信用のホップテーブルを伝送した（ステップＳ９）子機ＳＣとの間で周波数ホッピング方式による具体的な通信を開始する（ステップＳ１３）。

16

【００９５】そして、通信が終了したか否かが判定され（ステップＳ１４）終了していない時は（ステップＳ１４；ＮＯ）そのまま通信を継続し（ステップＳ１３）、終了している時は（ステップＳ１４；ＹＥＳ）、スリープ状態に移行する（ステップＳ１５）。そして親機ＳＯの電源が断とされたか否かが判定され（ステップＳ１６）、断とされた時（ステップＳ１６；ＹＥＳ）はそのまま処理を終了し、断とされていない時は（ステップＳ１６；ＮＯ）スリープ状態を継続する（ステップＳ１５）。

【００９６】次に、上記親機ＳＯの動作に対応した子機ＳＣのホップテーブル取得動作について、図２及び図５を用いて説明する。

【００９７】上記親機ＳＯの動作に対応して、新規接続されるべき子機ＳＣにおいては、始めに、上記ＩＤ情報（図４ステップＳ３参照）を送信し（ステップＳ２０）、次に、子機ＳＣのＲＡＭ１１に予め格納されている公開鍵に対応する上記公開鍵信号Ｓkoを送受信部２０を介して親機ＳＯに送信する（ステップＳ２１）。この公開鍵信号Ｓkoの送信では、上記テーブルｆを用いた周波数ホッピングが行われる。

【００９８】次に、送信した公開鍵信号Ｓkoに対応して親機ＳＯから送信されてきた（図４ステップＳ９参照）上記暗号化テーブル信号Ｓtaを受信する（ステップＳ２２）。そして、エラーなく受信できたか否かが判定され（ステップＳ２３）、受信できなかった時は（ステップＳ２３；ＹＥＳ）親機ＳＯに対して再送要求を行い（ステップＳ２４。図４ステップＳ１０参照）ステップＳ２２に戻って再送されてきた暗号化テーブル信号Ｓtaを受信する。

【００９９】一方、暗号化テーブル信号Ｓtaをエラーなく受信できた時は（ステップＳ２３；ＮＯ）、次に、ＲＡＭ３１に格納されている上記秘密鍵に対応する秘密鍵信号Ｓscを用いて、受信した暗号化テーブル信号Ｓtaを復号器３２において元のホップテーブルとして復元する（ステップＳ２５）。そして、暗号化テーブル信号Ｓtaの受信が完了したことを示す上記完了信号を親機ＳＯに送信し（ステップＳ２６。図４ステップＳ１１参照）、次にホップテーブルをそれまで使用していたテーブルｆから復元した無線通信用のホップテーブルに切り替え（ステップＳ２７）、当該親機ＳＯとの間で周波数ホッピング方式による具体的な通信を開始する（ステップＳ２８）。

【０１００】そして、通信が終了したか否かが判定され（ステップＳ２９）終了していない時は（ステップＳ２９；ＮＯ）そのまま通信を継続し（ステップＳ２８）、終了している時は（ステップＳ２９；ＹＥＳ）、スリープ状態に移行する（ステップＳ３０）。そして子機ＳＣの電源が断とされたか否かが判定され（ステップＳ３

１）、断とされた時（ステップＳ３１；ＹＥＳ）はそのまま処理を終了し、断とされていない時は（ステップＳ３１；ＮＯ）スリープ状態を継続する（ステップＳ３０）。

【０１０１】以上説明した第１実施形態の無線通信システムの動作によれば、授受すべき情報自体を秘匿化するためのホップテーブルを暗号化して親機ＳＯから子機ＳＣに送信し、子機ＳＣにおいて復元したホップテーブルを用いて情報を受信するので、周波数ホッピング方式による情報自体の秘匿化のみの場合に比して親機ＳＯと子機ＳＣ間の授受における情報の秘匿性が向上する。

【０１０２】また、予めホップテーブルを有しない子機ＳＣを新たに加えて情報の授受を開始する場合でも、授受のためのホップテーブルを暗号化して当該子機ＳＣに送信するので、ホップテーブルが外部に漏洩することがなく、情報の授受における秘匿性が向上する。

【０１０３】更に、周波数ホッピング方式におけるホップテーブルの授受を秘匿化して行うことにより盗聴等に対して情報を更に効果的に秘匿することができる。

【０１０４】また、公開鍵暗号システムを用いてホップテーブルを伝送するので、情報の秘匿性を更に向上させることができる。

【０１０５】なお、上述の方により子機ＳＣがホップテーブルを取得すれば、当該ホップテーブルが外部に漏洩することがないので、複数の子機ＳＣが親機に接続されている場合に、当該子機ＳＣ同士間での情報の授受の秘匿性も向上することとなる。

【０１０６】また、上記の実施形態においては、公開鍵信号Ｓko、暗号化テーブル信号Ｓtaを各インターフェースを介して取得する構成としたが、これに限らず、直接各コントローラを介して授受するようにしてもよい。

【０１０７】（II）第２実施形態

次に、本発明に係る他の実施形態である第２の実施形態について、図６及び図７を用いて説明する。ここで、図６は第２実施形態に係る親機ＳＯ’の構成を示す図であり、図７は第２実施形態に係る子機ＳＣ’の構成を示す図である。

【０１０８】上記の第１実施形態においては、子機ＳＣからの公開鍵を用いて親機ＳＯにおいてホップテーブル自体を暗号化し、これを子機ＳＣに送信して復元してホップテーブルを取得するようにしたが、第２実施形態においては、ホップテーブルを生成するための初期値のみを、子機ＳＣからの公開鍵を用いて親機ＳＯにおいて暗号化して子機ＳＣに送信し、当該子機ＳＣにおいて暗号化された初期値を用いてホップテーブルを生成する。

【０１０９】なお、図６及び図７において、夫々図１及び図２と同様の構成部材については同様の部材番号を付して細部の説明は省略する。

【０１１０】始めに、第２実施形態に係る親機ＳＯ’の構成について、図６を用いて説明する。

【０１１１】図６に示すように、第２実施形態に係る親機ＳＯ’は、第１実施形態におけるＲＡＭ１１に代えて、ホップテーブルを生成する際に用いられる初期値を格納する初期値格納部４０Ａを備えたＲＡＭ４０を備えていると共に、当該初期値を用いて無線通信用のホップテーブルを生成するホップテーブル生成器４１を備えている。その他の構成は上記親機ＳＯと同様である。

【０１１２】次に、第２実施形態に係る子機ＳＣ’の構成について、図７を用いて説明する。

【０１１３】図７に示すように、第２実施形態に係る子機ＳＣ’は、第１実施形態におけるＲＡＭ３１に代えて、上記初期値を格納する初期値格納部５０Ａを備えたＲＡＭ５０を備えていると共に、当該初期値を用いて無線通信用のホップテーブルを生成する生成手段としてのホップテーブル生成器５１を備えている。その他の構成は上記子機ＳＣと同様である。

【０１１４】次に、以上の構成を有する親機ＳＯ’及び子機ＳＣ’により構成される無線通信システムにおける第２実施形態の動作について説明する。

【０１１５】第２実施形態において新規な子機ＳＣ’を接続する際には、始めに当該子機ＳＣ’から親機ＳＯ’に対して上記公開鍵に対応する公開鍵信号Ｓkoを送信する。

【０１１６】そしてこれを受信した親機ＳＯ’においては、当該公開鍵を用いて予め格納されている初期値（接続しようとしている子機ＳＣ’との無線通信に用いられるべきホップテーブルを生成するための初期値）に対応する初期値信号Ｓiを暗号器１２において暗号化し、暗号化初期値信号Ｓiaを出力し、当該暗号化初期値信号Ｓiaを送受信部１を介して子機ＳＣ’に送信する。

【０１１７】一方、暗号化初期値信号Ｓiaを受信した子機ＳＣ’においては、送受信部２０を介して当該暗号化初期値信号Ｓiaを本体部３０’で取得し、これを上記秘密鍵信号Ｓscを用いて復号器３２において復元して元の初期値信号Ｓiを生成しＲＡＭ５０内の初期値格納部５０Ａに格納する。

【０１１８】次に、本来授受すべき情報の伝送の際には、親機ＳＯ’においては、予め格納されている初期値を用いてホップテーブル生成器４１においてホップテーブルを生成し、対応するテーブル信号ＳttをＰＬＬ９に出力して周波数ホッピングを行いつつ情報の授受を行う。

【０１１９】一方、子機ＳＣ’においては、親機ＳＯ’から送信され復元された初期値を初期値格納部５０Ａから取り出し、ホップテーブル生成器５１においてホップテーブルを生成し、対応するテーブル信号ＳttをＰＬＬ２８に出力して周波数ホッピングを行いつつ情報の授受を行う。

【０１２０】以上説明した第２実施形態の無線通信システムの動作によれば、初期値のみを暗号化して送信し、

これを受信した復号することにより、ホップテーブル自体を暗号化して親機から子機に送信する場合に比してより迅速に子機ＳＣ’においてホップテーブルを取得して送信されてきた情報を復号することができる。

【０１２１】なお、上記ホップテーブル生成器４１及び５１については、ソフトウェアを用いてコントローラ１４又は３４が機能することにより当該ホップテーブル生成器４１及び５１の機能を果たすようにしてもよい。また、所定の帰還タップを有するシフトレジスタを用いて充てることもできる。

【０１２２】（III）第３実施形態

次に、本発明に係る他の実施形態である第３の実施形態について、図８乃至図１１を用いて説明する。ここで、図８は第３実施形態に係る親機ＳＯ”の構成を示す図であり、図９は第３実施形態に係る子機ＳＣ”の構成を示す図である。また、図１０は第３実施形態における親機ＳＯ”の動作を示すフローチャートであり、図１１は第３実施形態における子機ＳＣ”の動作を示すフローチャートである。

【０１２３】上記の第１又は第２実施形態においては、周波数ホッピング方式のためのホップテーブルの取得を秘匿化する無線通信システムの実施形態について説明したが、本第３実施形態は、親機ＳＯ”に接続されようとしている子機が、予め設定登録されている子機ＳＣ”であるか否かを判断するためのいわゆるパスワードの授受を秘匿化するための無線通信システムについての実施形態である。

【０１２４】なお、図６及び図７において、夫々図１及び図２と同様の構成部材については同様の部材番号を付して細部の説明は省略する。

【０１２５】始めに、第３実施形態に係る親機ＳＯ”の構成について、図８を用いて説明する。

【０１２６】図８に示すように、第３実施形態に係る親機ＳＯ”は、第１実施形態における本体部１０に代えて、授受すべき情報を一時的に記憶すると共に、パスワードを格納するパスワード格納部６０Ａを備えたＲＡＭ６０と、後述の暗号化パスワード信号Ｓtwに基づいてパスワードを復元する復号器６１と、判断手段としての上述のコントローラ１４及び電源部１５を備えた本体部１０”を備えている。その他の構成は基本的に上記親機ＳＯと同様である。

【０１２７】次に、第３実施形態に係る子機ＳＣ”の構成について、図９を用いて説明する。

【０１２８】図９に示すように、第３実施形態に係る子機ＳＣ”は、第１実施形態における本体部３０に代えて、授受すべき情報を一時的に記憶すると共に、パスワードを格納するパスワード格納部７０Ａを備えたＲＡＭ７０と、後述の暗号化パスワード信号Ｓtwを生成する暗号器７１と、上述のコントローラ３４及び電源部３５を備えた本体部３０”を備えている。その他の構成は基本的に上記子機ＳＣと同様である。

【０１２９】次に、以上の構成を有する親機ＳＯ”及び子機ＳＣ”により構成される無線通信システムにおける第３実施形態のパスワード伝送動作について、図１０及び図１１を用いて説明する。なお、図１０に示すフローチャート及び図１１に示すフローチャートは、主としてコントローラ１４又は３４における処理を示すものである。

【０１３０】始めに、親機ＳＯ”における動作について、図８及び図１０を用いて説明する。

【０１３１】接続されている子機が予め設定登録されている子機ＳＣ”であるか否かを親機ＳＯ”において判定する際には、始めに、接続されている子機に対して同期信号及び公開鍵に対応する公開鍵信号Ｓkoを送信する（ステップＳ４０）。この場合には、予めＲＡＭ６０に格納されている公開鍵に対応する公開鍵信号Ｓkoを送信手段としての送受信部１を介して送信することとなる。このとき、上記テーブルｆ（図３（ｂ）参照）を用いて周波数ホッピング方式により送信するようにすることもできる。

【０１３２】公開鍵信号Ｓkoを送信すると、次に受信待機状態に移行し（ステップＳ４１）、接続されている子機からの呼出があったか否かが判定される（ステップＳ４２）。そして、呼出がない時は（ステップＳ４２；ＮＯ）、次に予め設定されている所定の時間が経過したか否かが判定され（ステップＳ４３）、経過していない時は（ステップＳ４３；ＮＯ）そのまま受信待機状態を継続し（ステップＳ４１）、所定時間が経過した時は（ステップＳ４３；ＹＥＳ）スリープ状態に移行する（ステップＳ４４）。そしてスリープ状態で更に予め設定された所定の時間が経過したか否かが判定され（ステップＳ４５）、経過していない時は（ステップＳ４５；ＮＯ）スリープ状態を継続し（ステップＳ４４）、経過した時は（ステップＳ４５；ＹＥＳ）、次に親機ＳＯ”の電源が断となっているか否かが判定され（ステップＳ４６）、断となっている時は（ステップＳ４６；ＹＥＳ）そのまま処理を終了し、断となっていない時は（ステップＳ４６；ＮＯ）再び公開鍵信号Ｓko等を送信すべくステップＳ４０に戻る。このステップＳ４３乃至Ｓ４６の処理により、受信待機時において所定の時間間隔をおいて同期信号及び公開鍵信号Ｓkoが繰返し送信されることとなる。

【０１３３】一方、ステップＳ４２の判断において、接続されている子機からの呼出があった時は（ステップＳ４２；ＹＥＳ）、当該子機からの上記ＩＤ情報を取得し（ステップＳ４７）、更に当該子機から送信されてくる後述の暗号化パスワード信号Ｓtwを送受信部１を介して取得し（ステップＳ４８）、当該暗号化パスワード信号Ｓtwを予めＲＡＭ６０に格納されている上記秘密鍵に対応する秘密鍵信号Ｓscを用いて復号器６１において復元

し、パスワード信号Ｓpwを得る（ステップＳ４９）。

【０１３４】次に、取得したパスワード信号Ｓpwがコントローラ１４に出力され、それが予め登録されている子機ＳＣ”を示すパスワード（当該パスワードは、無線伝送により外部から伝送されてきたものではなく、親機ＳＯ”自体を操作することにより設定されているものである。）に対応するものであるか否かが判定され（ステップＳ５０）、子機ＳＣ”を示すパスワードに対応するものでないときは（ステップＳ５０；ＮＯ）、接続されるべき子機ＳＣ”ではないとして接続されていた通信を切断し（ステップＳ５１）ステップＳ４０に戻る。

【０１３５】一方、子機ＳＣ”を示すパスワードに対応するものであるときは（ステップＳ５０；ＹＥＳ）、接続されている子機が子機ＳＣ”であるとして接続を許可する旨を当該子機ＳＣ”に対して送信し（ステップＳ５２）、次に子機ＳＣ”との間で具体的な通信を開始する（ステップＳ５３）。この時、上記無線通信用のホップテーブル（予め親機ＳＯ”及び子機ＳＣ”が備えているものとする。）を用いて周波数ホッピング方式により通信を行ってもよい。

【０１３６】そして、通信継続中において予め設定された所定時間が経過したか否かが判定され（ステップＳ５４）、経過していない時は（ステップＳ５４；ＮＯ）、次に通信自体が終了したか否かが判定され（ステップＳ５５）、終了している時は（ステップＳ５５；ＹＥＳ）、次の通信を行うべくステップＳ４０に戻り、通信が終了していない時は（ステップＳ５５；ＮＯ）そのまま継続する（ステップＳ５３）。

【０１３７】一方、ステップＳ５４の判定において、所定時間が経過した時は（ステップＳ５４；ＹＥＳ）、次にパスワードを再度送信する旨の要求信号（上記公開鍵信号Ｓkoを含む。）を子機ＳＣ”に送信し（ステップＳ５６）ステップＳ４７に戻る。このステップＳ５４及びＳ５６の動作により、通信継続中において所定時間毎にパスワードの確認が繰返されることとなる。

【０１３８】次に、上記親機ＳＯ”の動作に対応した子機ＳＣ”におけるパスワード伝送動作について、図９及び図１１を用いて説明する。

【０１３９】上記親機ＳＯ”の動作に対応して、パスワードを送信すべき子機ＳＣ”においては、始めに、親機ＳＯ”から送信されてきた（図１０ステップＳ４０参照）同期信号及び公開鍵信号Ｓkoを送受信部２０において受信し（ステップＳ６０）、次に受信した公開鍵信号Ｓkoを本体部３０”において取得してこれを用いて暗号器７１においてパスワード格納部７０Ａに格納されているパスワード（親機ＳＯ”において登録されているものと同じパスワードである。）に対応するパスワード信号Ｓiを暗号化し暗号化パスワード信号Ｓtwを生成する（ステップＳ６１）。ステップＳ６１における暗号化においては、第１又は第２実施形態と同様に、例えば、公開鍵暗号方式における、ＲＳＡ暗号、ＥlGamal暗号、楕円曲線暗号、楕円ＲＳＡ暗号又は逆数暗号等の暗号方式が用いられて暗号化が行われる。

【０１４０】次に、親機ＳＯ”に対して呼出信号を送信し（ステップＳ６２。図１０ステップＳ４２参照）、続いて当該子機ＳＣ”の上記ＩＤ情報を送信する（ステップＳ６３。図１０ステップＳ４７参照）。

【０１４１】続いて上記暗号化パスワード信号Ｓtwを送受信部２０を介して送信する（ステップＳ６４。図１０ステップＳ４８参照）。この時、上記テーブルｆを用いて周波数ホッピング方式により送信してもよい。

【０１４２】次に、親機ＳＯ”からの上記接続許可信号を受信したら（ステップＳ６５。図１０ステップＳ５２参照）、親機ＳＯ”との間で具体的な通信を開始する（ステップＳ６６。図１０ステップＳ５３参照）。この時、上記無線通信用のホップテーブルを用いて周波数ホッピング方式により通信を行ってもよい。

【０１４３】次に、親機ＳＯ”より定期的なパスワードの送信要求（図１０ステップＳ５６参照）があったか否かが判定され（ステップＳ６７）、あった場合には（ステップＳ６７；ＹＥＳ）上記ステップＳ６１及びＳ６４の処理を行って暗号化パスワード信号Ｓtwを親機ＳＯ”に送信して通信を継続すべくステップＳ６６に戻る。

【０１４４】一方、ステップＳ６７の判定において、パスワードの送信要求がない場合には（ステップＳ６７；ＮＯ）、次に通信が終了したか否かが判定され（ステップＳ６８）、終了していない時は（ステップＳ６８；ＮＯ）そのまま通信を継続し（ステップＳ６６）、終了している時は（ステップＳ６８；ＹＥＳ）スリープ状態に移行する（ステップＳ６９）。そして子機ＳＣ”の電源が断となったか否かが判定され（ステップＳ７０）、断となっていない時は（ステップＳ７０；ＮＯ）そのままスリープ状態を継続し（ステップＳ６９）、断となった時は（ステップＳ７０；ＹＥＳ）処理を終了する。

【０１４５】以上説明した第３実施形態の無線通信システムの動作によれば、パスワードを暗号化して親機ＳＯ”に送信し、これを復号するので、パスワードが外部に知得されることがなく、確実に接続されるべき子機ＳＣ”を識別して情報の授受を行うことができる。

【０１４６】また、公開鍵暗号方式を用いて暗号化するので、パスワード及びその後の情報の授受の秘匿性を更に向上させることができる。

【０１４７】なお上述の第３実施形態において、親機ＳＯ”からの一定時間毎のパスワード送信要求信号（図１０ステップＳ５６参照）中に含まれる公開鍵を、要求信号の度に毎回変更するようにすれば、更にパスワードの秘匿性は向上することとなる。

【０１４８】更に、親機ＳＯ”において子機ＳＣ”からのＩＤ情報を受け取った（図１０ステップＳ４７参照）後に、例えば、乱数を子機ＳＣ”に送信し、これを受信

した子機ＳＣ”がパスワードに乱数を加算したものを親機ＳＯ”からの公開鍵を用いて暗号化し（図１１ステップＳ６４参照）親機ＳＯ”に送信するようにすると共に、これを受信した親機ＳＯ”において秘密鍵で復元する（図１０ステップＳ４９参照）と共に乱数を差し引いてパスワードを取得するように構成することもできる。このようにすれば、子機ＳＣ”が親機ＳＯ”に対して送信する暗号化パスワード信号Ｓtwの内容が毎回異なることとなり、パスワードの秘匿性が更に向上する。

【０１４９】更にまた、上述の各実施形態においては、情報の授受に関する部分のみ説明したが、各実施形態の無線通信システムにより授受されるべき情報は、例えば、ファクシミリ送受信されるべきファクシミリ情報であってもよいし、電話により送受信されるべき音声情報であってもよい。更にコンピュータとプリンタ（又はファクシミリ装置等）間において授受されるべき情報であってもよい。この場合には、各実施形態における親機又は子機が、夫々ファクシミリ、電話機又はコンピュータとプリンタに搭載されることとなる。そして、各実施形態におけるインターフェースの構成については、親機又は子機が電話機に備えられている時は音声とディジタル情報との相互変換を行うコーデック及び圧縮器から構成されており、また、親機又は子機においてコンピュータ等の情報を取扱う時はバッファやエラー訂正処理を行うデータ変換器等より構成される。

【０１５０】更に、上述の実施形態における暗号化テーブル信号Ｓta、暗号化初期値信号Ｓia又は暗号化パスワード信号Ｓtwの伝送は、新たに子機を登録するときのみ登録モードとして行ってもよいし、通信開始時に毎回行うようにしてもよい。

【０１５１】また、通信中に適時ホップテーブルの生成のための生成情報を伝送し、更に秘匿性を高めるようにしてもよい。

【０１５２】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、授受すべき情報自体を秘匿化するための秘匿化情報を暗号化して親機から子機に送信し、子機において復元した秘匿化情報を用いて秘匿化を解除しつつ情報を取得するので、情報自体の秘匿化のみの場合に比して親機と子機間又は子機同士間の授受における情報の秘匿性が向上する。

【０１５３】また、予め秘匿化情報を有しない子機を新たに加えて情報の授受を開始する場合でも、授受のための秘匿化情報を暗号化して当該子機に送信するので、秘匿化情報が外部に漏洩することがなく、情報の授受における秘匿性が向上する。

【０１５４】請求項２に記載の発明によれば、暗号鍵情報に基づいて識別情報を暗号化して送信し、これを受信して復元した後に設定子機か否かを判別するので、識別情報が外部に知得されるがことなく、確実に設定子機を識別して情報の授受を行うことができる。

【０１５５】従って、設定子機以外の子機に対して情報が伝達されることを防止でき、情報の秘匿性を更に高めることができる。

【０１５６】請求項３に記載の発明によれば、授受すべき情報自体を秘匿化するための秘匿化情報を暗号化して親機から子機に送信し、子機において復元した秘匿化情報を用いて秘匿化を解除しつつ情報を取得するので、情報自体の秘匿化のみの場合に比して親機と子機間又は子機同士間の授受における情報の秘匿性が向上する。

【０１５７】また、予め秘匿化情報を有しない子機を新たに加えて情報の授受を開始する場合でも、授受のための秘匿化情報を暗号化して当該子機に送信するので、秘匿化情報が外部に漏洩することがなく、情報の授受における秘匿性が向上する。

【０１５８】請求項４に記載の発明によれば、請求項３に記載の発明の効果に加えて、情報の秘匿化が当該情報の授受に用いられる周波数を時間的に変化させて行われると共に、秘匿化情報が周波数を変化させる時に参照されるテーブル情報であるので、テーブル情報の授受を秘匿化して行うことにより盗聴等に対して情報を更に効果的に秘匿することができる。

【０１５９】請求項５に記載の発明によれば、請求項３又は４に記載の発明の効果に加えて、暗号鍵情報が公開鍵暗号システムにおける公開鍵であると共に、復号鍵情報が公開鍵暗号システムにおける秘密鍵であるので、更に情報の秘匿性を向上させることができる。

【０１６０】請求項６に記載の発明によれば、請求項４又は５に記載の発明の効果に加えて、秘匿化情報は周波数を変化させる時に参照されるテーブル情報を生成するための生成情報であると共に、子機が当該生成情報を用いてテーブル情報を生成するための生成手段を更に備えるので、テーブル情報自体を秘匿化情報として暗号化して親機から子機に送信する場合に比してより迅速に子機においてテーブル情報を取得して送信されてきた情報を復号することができる。

【０１６１】請求項７に記載の発明によれば、暗号鍵情報に基づいて識別情報を暗号化して送信し、これを受信して復元した後に設定子機か否かを判別するので、識別情報が外部に知得されることがなく、確実に設定子機を識別して情報の授受を行うことができる。

【０１６２】従って、設定子機以外の子機に対して情報が伝達されることを防止でき、情報の秘匿性を更に高めることができる。

【０１６３】請求項８に記載の発明によれば、請求項７に記載の発明の効果に加えて、暗号鍵情報が公開鍵暗号システムにおける公開鍵であると共に、復号鍵情報が公開鍵暗号システムにおける秘密鍵であるので、更に情報の秘匿性を向上させることができる。

【図面の簡単な説明】

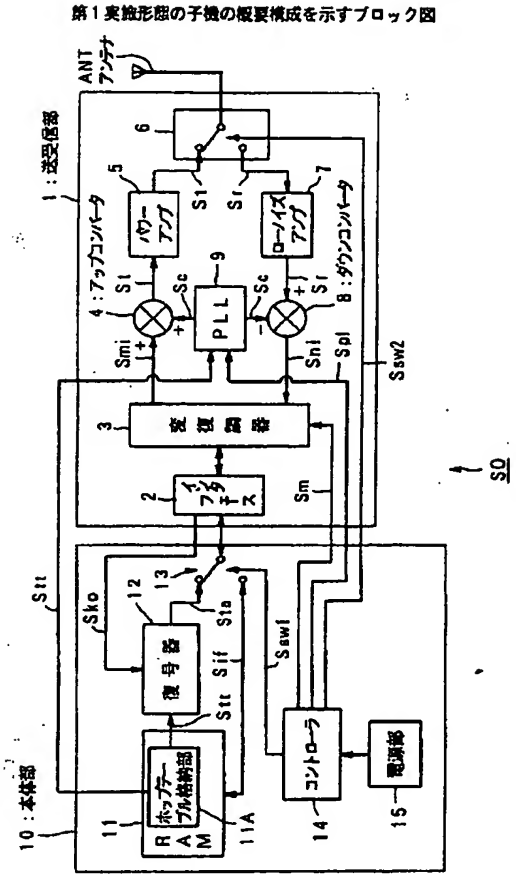
25

【図１】第１実施形態の親機の概要構成を示すブロック図である。
【図２】第１実施形態の子機の概要構成を示すブロック図である。
【図３】フレームの構成及びホップテーブルの一例を示す図であり、（ａ）はフレームの構成を示す図であり、（ｂ）はホップテーブルの一例を示す図である。
【図４】第１実施形態の親機の動作を示すフローチャートである。
【図５】第１実施形態の子機の動作を示すフローチャートである。
【図６】第２実施形態の親機の概要構成を示すブロック図である。
【図７】第２実施形態の子機の概要構成を示すブロック図である。
【図８】第３実施形態の親機の概要構成を示すブロック図である。
【図９】第３実施形態の子機の概要構成を示すブロック図である。
【図１０】第３実施形態の親機の動作を示すフローチャートである。
【図１１】第３実施形態の子機の動作を示すフローチャートである。
【符号の説明】
１、２０…送受信部
２、２１…インタフェース
３、２２…変復調器
４、２３…アップコンバータ
５、２４…パワーアンプ
６、２５…送受切替スイッチ
７、２６…ローノイズアンプ
８、２７…ダウンコンバータ
９、２８…ＰＬＬ
１０、３０、１０’、３０’、１０”、３０”…本体部

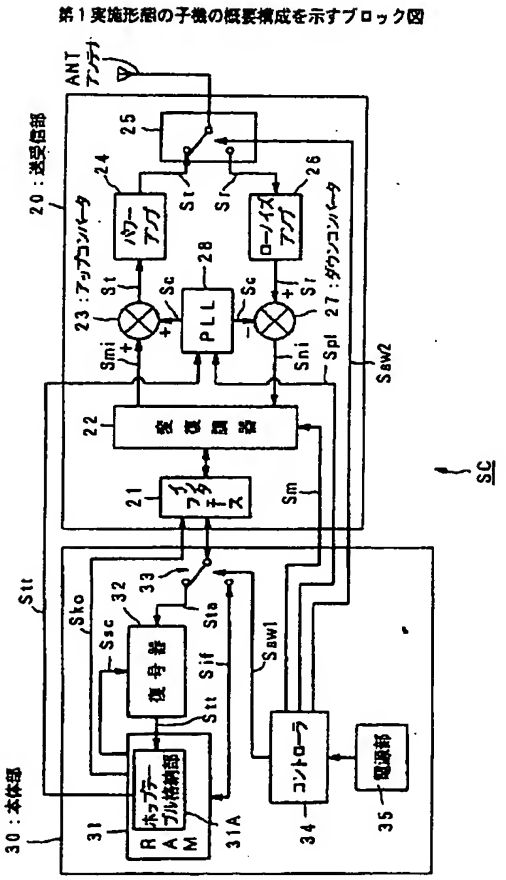
26

１１、３１、４０、５０、６０、７０…ＲＡＭ
１１Ａ、３１Ａ…ホップテーブル格納部
１２…暗号器
１３、３３…切替スイッチ
１４、３４…コントローラ
１５、３５…電源部
１６、１７…フレーム
１６Ａ、１７Ａ…周波数ホップフェーズブロック
１６Ｂ、１７Ｄ…送信フェーズブロック
１６Ｃ、１７Ｃ…送受切替フェーズブロック
１６Ｄ、１７Ｂ…受信フェーズブロック
３２…復号器
４０Ａ、５０Ａ…初期値格納部
４１、５１…ホップテーブル生成器
６０Ａ、７０Ａ…パスワード格納部
ＳＯ、ＳＯ’、ＳＯ”…親機
ＳＣ、ＳＣ’、ＳＣ”…子機
Ｓtt…テーブル信号
Ｓif…情報信号
Ｓta…暗号化テーブル信号
Ｓko…公開鍵信号
Ssw_1、Ssw_2、Ｓm、Ｓpl…制御信号
Ｓc…局部信号
Ｓt…送信信号
Ｓr…受信信号
Ｓmi…変調信号
Ｓni…復調信号
Ｓsc…秘密鍵信号
Ｓi…初期値信号
Ｓia…暗号化初期値信号
Ｓpw…パスワード信号
Ｓtw…暗号化パスワード信号
ＡＮＴ…アンテナ

【図１】

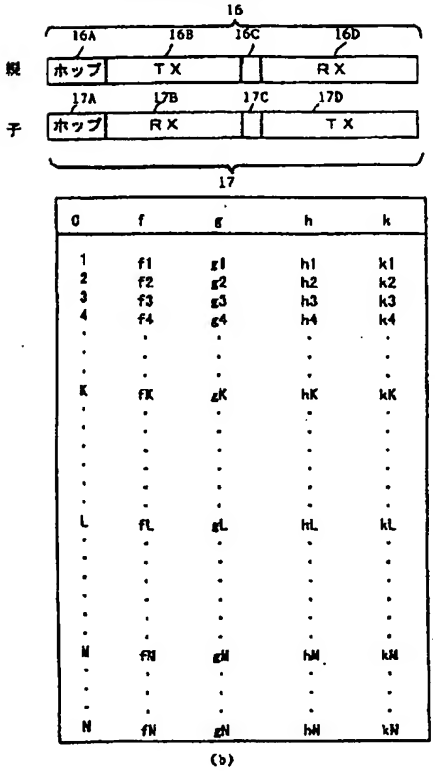

第１実施形態の子機の概要構成を示すブロック図
ANT
アンテナ
1：送受信部
4：アップコンバータ
8：ダウンコンバータ
パワーアンプ
ローノイズアンプ
PLL
変復調器
インタフェース
復号器
ホッタープル格納部
RAM
コントローラ
電源部
10：本体部
SO

【図２】


第１実施形態の子機の概要構成を示すブロック図
ANT
アンテナ
20：送受信部
23：アップコンバータ
27：ダウンコンバータ
パワーアンプ
ローノイズアンプ
PLL
変復調器
インタフェース
復号器
ホッタープル格納部
RAM
コントローラ
電源部
30：本体部
SC

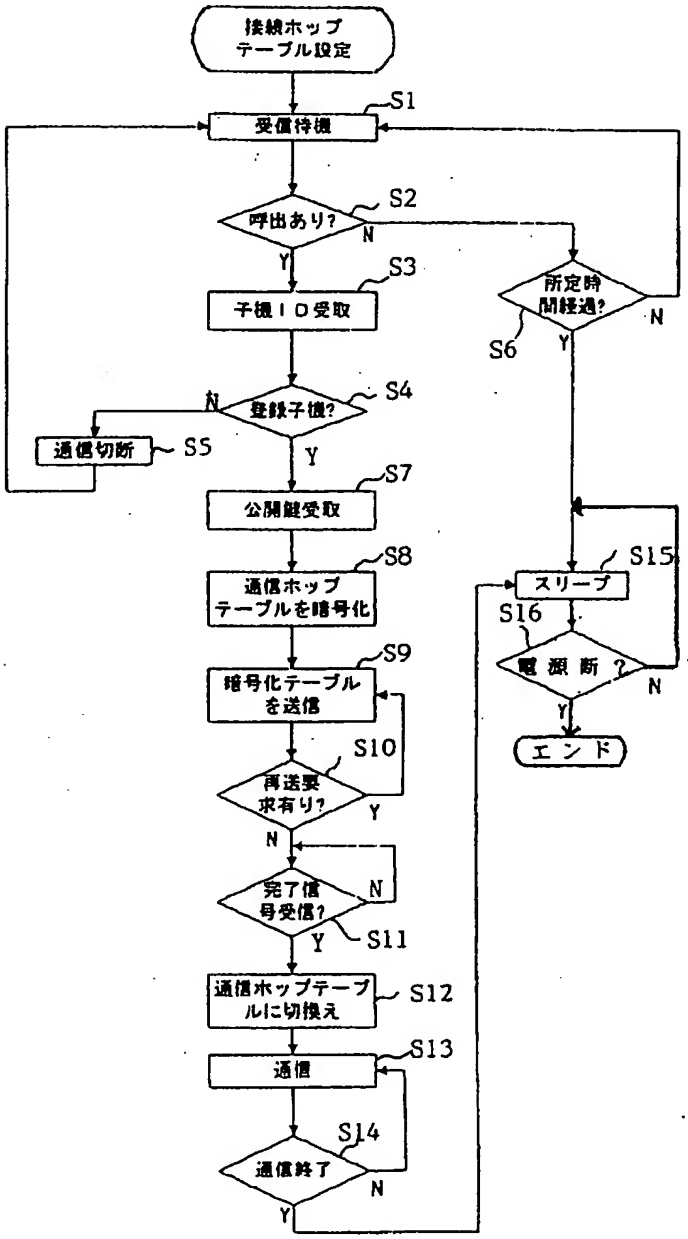
【図３】

フレームの構成及びホップテーブルの一例



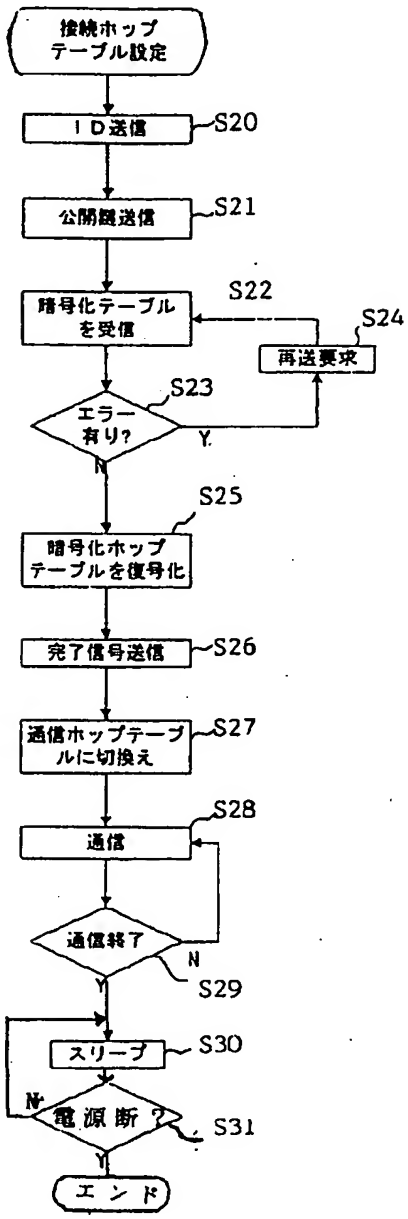
【図４】

第１実施形態の親機の動作を示すフローチャート



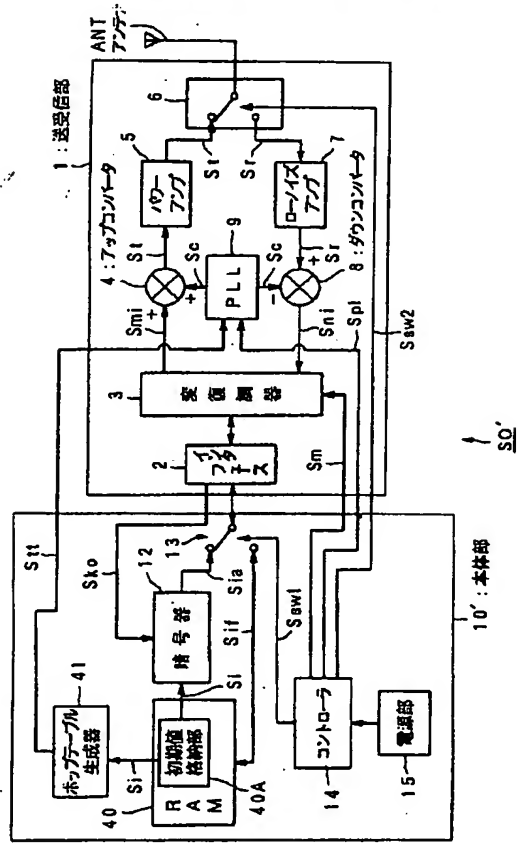
【図５】

第１実施形態の子機の動作を示すフローチャート

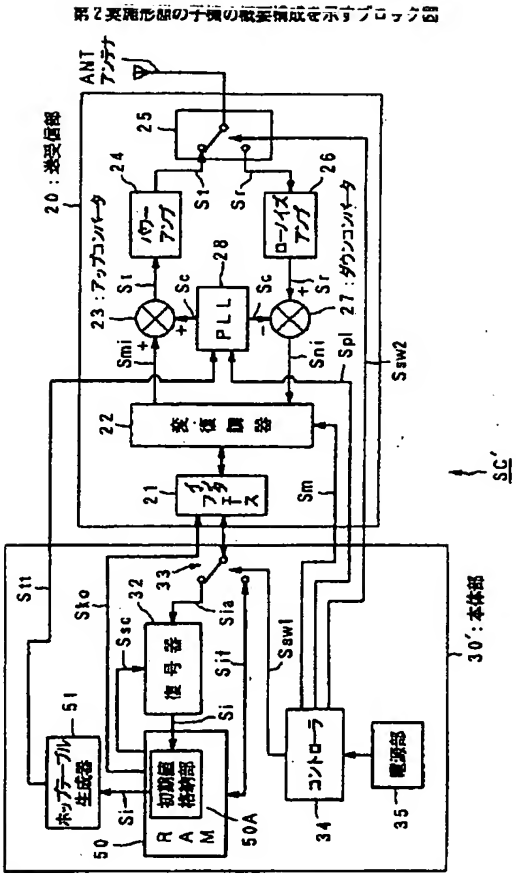


【図６】

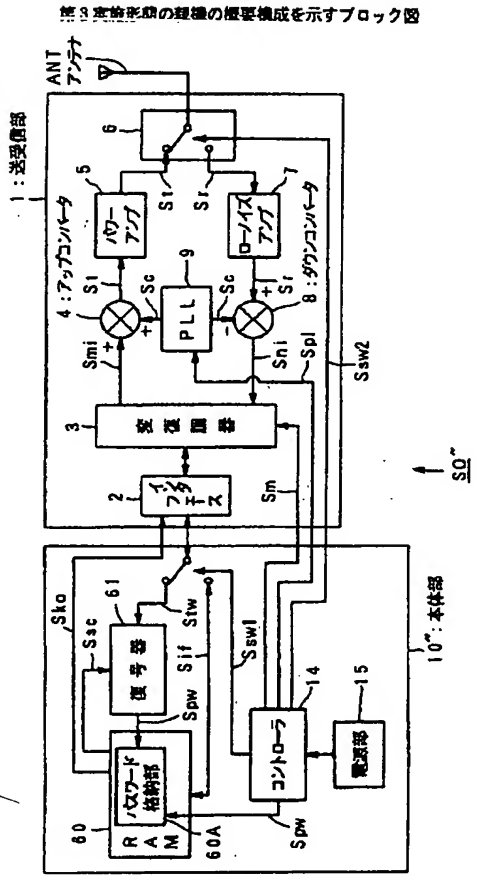
第２実施形態の親機の概要構成を示すブロック図



【図７】

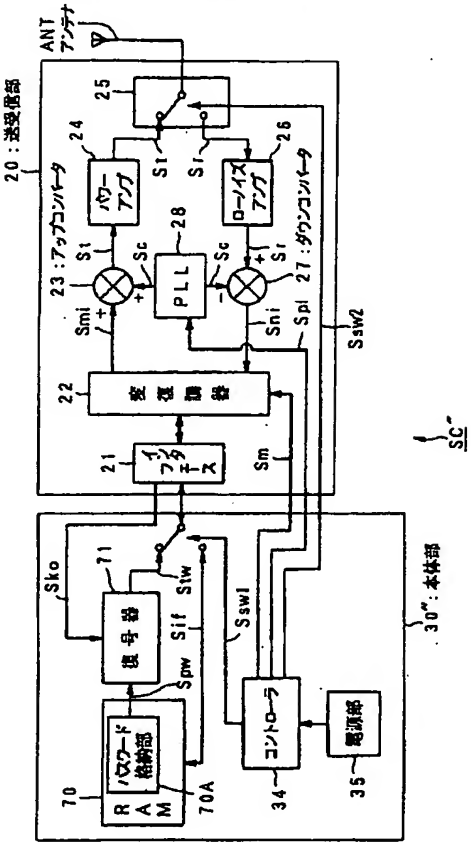

第２実施形態の子機の概要構成を示すブロック図
ANT
アンテナ
20：送受信部
25
24
パワーアンプ
26
ローノイズアンプ
23：アップコンバータ
28
PLL
27：ダウンコンバータ
Smi
Sni
Spl
Ssw2
22
変復調器
21
インターフェース
Sm
SC'
Stt
Sto
32
33
Ssc
復号器
Sia
Sif
Si
Ssw1
51
ホップテーブル生成器
初期値格納部
RAM
50
50A
コントローラ
34
電源部
35
30'：本体部

【図８】


第３実施形態の親機の概要構成を示すブロック図
ANT
アンテナ
1：送受信部
6
5
パワーアンプ
7
ローノイズアンプ
4：アップコンバータ
9
PLL
8：ダウンコンバータ
Smi
Sni
Spl
Ssw2
3
変復調器
2
インターフェース
Sm
SC"
Sko
Ssc
61
復号器
Stw
Sif
Spw
Ssw1
パスワード格納部
RAM
60
60A
14
コントローラ
15
電源部
10"：本体部

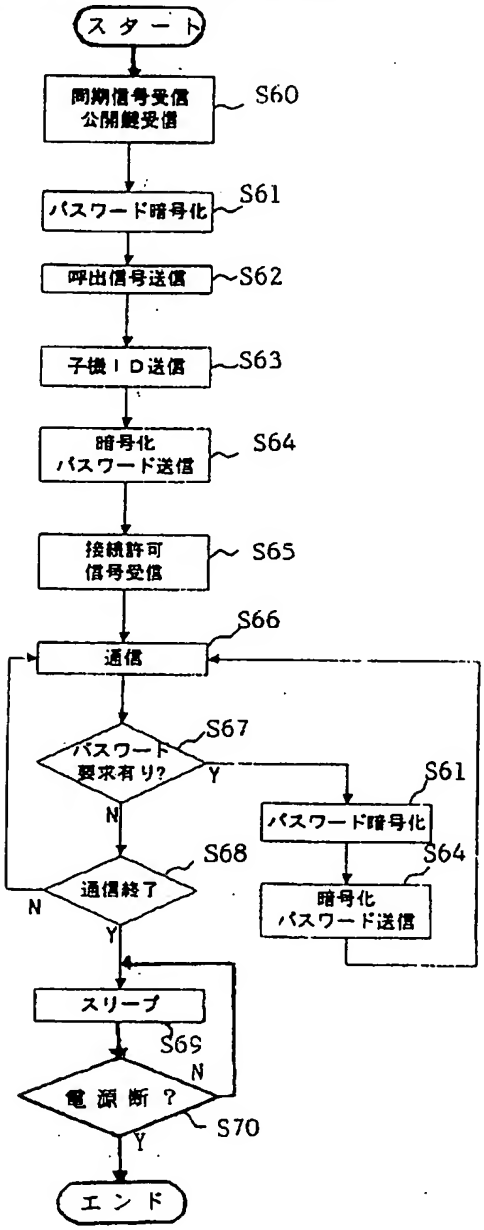
【図９】

第３実施形態の子機の概要構成を示すブロック図



【図１１】

第３実施形態の子機の動作を示すフローチャート



【図１０】

第３実施形態の親機の動作を示すフローチャート